UNIVERSIDAD CENTROAMERICANA

(UCA)

Facultad de Ciencias Económicas y Empresariales

Trabajo de Investigación para obtener el título de Master en Economía con mención en Finanzas

“Riesgo Operacional en la Banca y su Administración en Nicaragua”

Autor: **Lic. Snizhana Lipova**

Tutor: **Msc. Ernesto Huezo Castillo**

Managua, Nicaragua 24 de Agosto 2010

TEMA: **“Riesgo Operacional en la Banca y su Administración en Nicaragua”**

Resumen

El riesgo operacional, según la definición del Comité de Supervisión Bancaria de Basilea (BCBS), es el riesgo de pérdidas resultantes de la inadecuación o fallas en los procesos internos, las personas, los sistemas o por eventos externos; esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y reputacional. Tradicionalmente las instituciones financieras han gestionado por aparte cada uno de estos riesgos para evitar el fraude y mantener la integridad de sus controles internos. Sin embargo recientemente el BCBS ha considerado a la gestión del riesgo operacional como una práctica integral comparable a la gestión de otros riesgos e introdujo distintas metodologías para medir las pérdidas provenientes de eventos de riesgo operacional.

En Nicaragua la gestión del riesgo operacional es un tema reciente, donde la Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF) apenas desde el año 2006 empezó a introducir las normativas regulatorias relacionadas, y a partir del mes de enero del año en curso aprobó una norma específica para la gestión del riesgo operacional, prevista a entrar en plena vigencia en el mes de agosto.

Este documento describe los estándares internacionales del riesgo operacional propuestos en cuanto a los conceptos generalmente aceptados, destaca la importancia de gestión del riesgo operacional, sus fuentes, elementos, etapas y métodos de medición. Así mismo, reúne las normas dictadas por la SIBOIF de Nicaragua para la gestión del riesgo operacional en la banca y presenta los avances en su aplicación en la práctica por parte de las instituciones financieras del país.

Índice

Abreviaturas

ALMA: Advanced Measurement Approach (Métodos de Medición Avanzada)

BCBS: Comité de Supervisión Bancaria de Basilea

BIA: Basic Indicator Approach (Método de Indicador Básico)

EIF: Entidades de Intermediación Financiera

GRHH: Gerencia de Recursos Humanos

IMA: Internal Measurement Approach (Modelos de Medición Interna)

JD: Junta Directiva

LDA: Loss Distribution Approach (Modelos de Distribución de Pérdidas)

SA: Standardized Approach (Método Estándar)

SIBOIF: Superintendencia de Bancos y de Otras Instituciones Financieras

TI: Tecnologías de Información

UAIR: Unidad de Administración Integral de Riesgos

"Aquel que está preparado y espera lo inesperado será victorioso"
Sun Tsu

I. INTRODUCCION

En los últimos años en los círculos financieros de la banca internacional, así como por parte de los supervisores y reguladores de la actividad bancaria de los países, ha salido a la luz la preocupación sobre el tratamiento del riesgo operacional, un riesgo que siempre ha existido, sin embargo en actualidad se manifiesta con una mayor intensidad, debido a factores como la creciente complejidad del negocio bancario, evolución de los sistemas tecnológicos y la globalización del sistema financiero en general.

Grandes fraudes y estafas causadas por una inadecuada gestión del riesgo operacional por fallos de sistemas, falta de segregación de funciones, falta de controles o controles inadecuados, malas prácticas con clientes, etc., han generado importantes pérdidas a instituciones financieras, llevando a algunas a la quiebra. Así mismo, los factores externos que son ajenos a la funcionabilidad interna de un banco, como desastres naturales, actos terroristas y vandalismo, han generado daños a la estructura física de los bancos, interrumpiendo temporalmente la operatividad de los mismos.

Por tanto, si bien es cierto que la presencia del riesgo forma parte constante de la operatividad en el mundo financiero de la banca, es necesaria su adecuada administración, control y gestión, para minimizar las posibles pérdidas o bien, evitarlas o mitigarlas; afectando en la menor medida posible su capital.

Las entidades financieras han incrementado paulatinamente los recursos asignados al manejo del riesgo operacional, pasando de la simple mejora de los sistemas de control al desarrollo de modelos de medición y gestión, intentando obtener una estimación razonable del impacto de futuras pérdidas.

El Comité de Basilea, el organismo internacional de supervisión bancaria, ha venido trabajando durante varios años sobre el tema y finalmente estableció un nuevo marco regulatorio que reorienta el enfoque tradicional de control interno hacia un concepto más amplio, incluyendo el riesgo operacional dentro de las exigencias de capital,

señalando que cada entidad financiera deberá contar con el capital necesario en función de su perfil de riesgo.

Los países miembros de este comité, así como otros, incluyendo Nicaragua, han seguido gradualmente sus recomendaciones en materia de las regulaciones bancarias, y concretamente en cuanto al tratamiento del riesgo operacional, introduciendo la legislación relacionada y dictaminando las normas de obligatorio cumplimiento para los bancos a nivel nacional, contribuyendo a la solidez de los sistemas financieros.

De esta manera, el propósito del este trabajo investigativo es exponer sobre las principales tendencias en la temática del riesgo operacional que están propuestas en materia de supervisión bancaria a nivel internacional: la conceptualización del riesgo operacional, diferenciación entre los distintos tipos de riesgo a cuales está expuesta la actividad financiera; destacar la importancia de gestión del riesgo operacional, sus fuentes, elementos y etapas. Así mismo, una vez presentadas las recomendaciones internacionales en materia, informar sobre las recientes acciones tomadas en Nicaragua en cuanto a la regulación del riesgo operacional y los avances en su aplicación en la práctica por parte de las instituciones financieras del país.

Para la realización del presente trabajo se utilizó el método de investigación documental, recopilando la información internacional disponible en materia de riesgo operacional, lo que incluye las publicaciones sobre el tema, legislación, tanto internacional, como nacional; así mismo con el fin de conocer sobre los avances en la gestión del riesgo operacional en Nicaragua, se efectuó la entrevista al personal de la Dirección de Normas de la Superintendencia de Bancos y de otras Instituciones Financieras.

II. DESARROLLO

2.1 Conceptualización del riesgo.

Es frecuente encontrar que el término riesgo se usa como sinónimo de peligro. Según la Real Academia Española la palabra riesgo implica la proximidad de un daño, desgracia o contratiempo que puede afectar la vida de los hombres (Real Academia Española, 1992, p.1.562). Este término, muy empleado en Economía, Política y Medicina, ha extendido su uso a todas las ciencias.

El origen del término riesgo es incierto; según Díez y otros lingüistas, se relaciona con el castellano antiguo resegue (resecar, cortar), cuya acepción, muy usada en la Edad Media, es sinónimo de lucha, contradicción y división. Por ello se piensa que probablemente todo el grupo riesgo-risco procede del latín resecare, cortar, que tiene doble acepción: por un lado división, discordia y por otro, lugar quebrado y fragoso. Etimológicamente riesgo proviene de rísico o rischio (peligro).

Por otra parte, por ejemplo, en epidemiología el concepto de riesgo tiene un sentido diferente, matemático, o sea, la probabilidad de que un evento ocurra o no, combinando la magnitud de las pérdidas y ganancias involucradas en la acción realizada.

Los riesgos implican un mayor grado de controversia científica que los peligros, tanto respecto de sus causas como de sus consecuencias y probabilidades de ocurrencia[1]. La acepción más divulgada de riesgo es la de peligro que se corre. El concepto de riesgo incluye la probabilidad de ocurrencia de un acontecimiento natural o antrópico y la valoración por parte del hombre en cuanto a sus efectos nocivos (vulnerabilidad). La valoración cualitativa puede hacerse cuantitativa por medición de pérdidas y probabilidad de ocurrencia. Cuando se cuenta con los datos adecuados para realizar un cálculo de probabilidades se puede definir el riesgo. En cambio, cuando no existe

[1] Los primeros estudios serios sobre probabilidad se desarrollaron en la época de Renacimiento, el siglo XVI con los múltiples trabajos escritos por los italianos Girolamo Cardado (1500-1571) y Galileo (1564-1642), los siguieron en el siglo XVII otros personajes que propusieron un método sistemático para medir la probabilidad (franceses Blas Pascal, Pierre de Fermat y Chevalier de Meré).

posibilidad de calcular probabilidades, sino que solo existe intuición o criterio personal, se está frente a una incertidumbre. [2]

Transcurriendo las épocas, con el desarrollo científico y tecnológico, las sociedades aprendieron identificar los peligros, esquivarlos o administrarlos, previniendo los posibles daños que pudiesen habido ocasionarles o minimizando los daños recibidos.

La Economía y particularmente la Actividad Bancaria, no son ajenas a las estimaciones de los riesgos implícitos, debido a que todas las decisiones que se toman implican cierto grado de incertidumbre o riesgo. Por lo tanto es importante saber identificarlo y administrarlo para la buena marcha del negocio, minimizando las posibles pérdidas.

2.2 Clasificación de los riesgos.

Los riesgos que afecten a las actividades financieras pueden clasificarse por su alcance o por su naturaleza.

Según su alcance, el riesgo puede ser sistémico (cuando un evento afecta a todo el sistema financiero) y no-sistémico (también denominado específico, cuando un evento afecta individualmente a una entidad bancaria). La diferencia entre ambos es que en el primer caso, el riesgo no puede reducirse mediante la diversificación, como por ejemplo un evento político, mientras que los riesgos no-sistémicos pueden reducirse a través de diversificación.

Según la naturaleza de las operaciones se puede señalar los siguientes más comunes de los riesgos financieros:

- *Riesgo de Crédito:* es el más antiguo de los riesgos que enfrentan los bancos y se puede definirse como la pérdida potencial que asume un banco como consecuencia del incumplimiento de las obligaciones contractuales por parte de un tercero. En otras palabras es el riesgo de no recuperar completamente o en parte los recursos otorgados a un tercero, ya sea por razones de que este último

[2] Susana D. Aneas de Castro “RIESGOS Y PELIGROS: UNA VISIÓN DESDE LA GEOGRAFÍA” *Scripta Nova. Revista Electrónica de Geografía y Ciencias Sociales*. Universidad de Barcelona [ISSN 1138-9788]. Nº 60, 15 de marzo de 2000.

no tenga capacidad de pago o no quiera cumplir con los compromisos de pago estipulados en el contrato.

En la mayoría de las entidades financieras, según la composición del activo, la cartera de préstamos es la principal fuente de riesgo de crédito; sin embargo, otras actividades también conllevan este riesgo, entre las cuales están las inversiones permanentes, los depósitos en otras instituciones financieras y las actividades fuera de balance (operaciones contingentes y otros).

Las entidades que otorgan préstamos o compran inversiones a un plazo más largo están más expuestas al riesgo de crédito que aquellas cuyos préstamos e inversiones tienen un vencimiento más corto. No existiría riesgo de crédito si todos los préstamos e inversiones fueran cobrados en su totalidad en los términos y plazos originalmente pactados, sin embargo esta situación en la realidad es poco probable, estando siempre presente el riesgo de crédito en mayor o menor grado. Por otra parte, si el prestatario o contraparte quiebra o presenta debilidades financieras, el riesgo de crédito se incrementa, poniendo en duda la recuperación del capital.

- *Riesgo de Mercado:* es el riesgo resultante de variaciones en los precios de mercado de los instrumentos financieros en poder de la entidad bancaria. Esta categoría incluye el Riesgo Cambiario (posibilidad o probabilidad de sufrir pérdidas por fluctuaciones en los tipos de cambio de las monedas en las que están denominados los activos, pasivos y operaciones fuera de balance de la entidad) y el Riesgo de Tasa de Interés (la posibilidad o probabilidad de que se incurra en pérdidas como consecuencia de movimientos adversos de las tasas de interés, sean estas fijas o variables). Así mismo el riesgo de mercado está asociado con las fluctuaciones en los precios de los valores de renta variable (equities) y precios de las materias primas (commodities).

- *Riesgo de Liquidez:* es el riesgo que tenga una entidad financiera bancaria de no tener suficientes activos líquidos para honrar sus obligaciones o retiros de depósitos en un momento determinado. También lo llaman el riesgo de

financiación ya que se refiere a la imposibilidad de transformar en efectivo un activo o portafolios, o sea la imposibilidad de vender un activo en el mercado en un momento de crisis. Así como la posibilidad o probabilidad de sufrir pérdidas por la venta anticipada o forzosa de activos a descuentos inusuales y/o significativos, con el fin de disponer rápidamente de los recursos necesarios para cumplir con sus compromisos, o por la imposibilidad de renovar o de contratar nuevos financiamientos en condiciones normales para la entidad.

El riesgo de liquidez se relaciona con los riesgos del mercado ya que los activos y pasivos están nominados por el tipo de moneda y porque los instrumentos líquidos negociables se contratan a una determinada tasa de interés. Así mismo el riesgo de liquidez está estrechamente relacionado con la rentabilidad del banco debido a que el hecho de almacenar los recursos líquidos o conseguir el financiamiento para disponer de efectivo en un momento dado puede implicar menor margen financiero.

- *Riesgo Operacional u Operativo:* a diferencia de otros tipos de riesgos financieros antes mencionados, el presente riesgo es más amplio, debido a que envuelve tanto factores externos, como internos de la propia organización bancaria y es un riesgo que no se toma voluntariamente como el resto, sino que viene implícito en la operatividad de la empresa. Se refiere a la posibilidad de incurrir en pérdidas por deficiencias o fallas en el recurso humano, los procesos, la tecnología e infraestructura, así como por la ocurrencia de acontecimientos extremos externos. Dicho riesgo incluye el riesgo legal, pero excluye el riesgo reputacional y la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.

- *Riesgo Legal:* Es la eventualidad de pérdida en que puede incurrir la entidad financiera al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. De igual forma el riesgo legal puede surgir como consecuencia de fallas en los contratos y transacciones donde los derechos u obligaciones de las partes no están bien

definidos, así como las actuaciones malintencionadas, negligencia o actos involuntarios que afecten la ejecución de los contratos o transacciones.

- *Riesgo Reputacional:* Es el riesgo de que se forme una opinión pública negativa sobre el servicio bancario prestado o sobre el banco en particular. El riesgo reputacional puede derivar en acciones que fomenten la creación de una mala imagen o un posicionamiento negativo en la mente de los clientes, de tal forma que se produzca una migración de fondos hacia otras entidades debido a una pérdida de credibilidad, lo que se transformaría a su vez en pérdidas financieras y es un riesgo de liquidez para un determinado banco por no poder concretar las oportunidades de negocio atribuibles a un desprestigio ante los ojos de los clientes, ya sea por falta de capacitación del personal, fraudes o errores en algún proceso de operación.

2.3 Fuentes del Riesgo Operacional y sus Elementos.

El Riesgo Operacional, la temática a ser abordada en la presente investigación, se puede dividir en dos grandes grupos: el primero de los cuales engloba los riesgos internos relacionados principalmente con personas, procesos y sistemas; y en otro grupo se ubican los riesgos externos.

Personas: son todas las posibles pérdidas que pueden ser asociadas con errores de los empleados, negligencias en el desempeño de sus funciones, falsificaciones, fraudes o sabotajes por parte de los empleados (por ejemplo negociaciones fraudulentas en las cuentas del banco, blanqueo de capitales), utilización de información confidencial en beneficio del mismo empleado o en perjuicio de los clientes. También en esta categoría se incluyen las pérdidas eventuales por pérdida del personal clave, o al contrario por falta de conocimiento/ habilidades del personal, así como la falta institucional de capacitación del mismo. Por otra parte, las situaciones ligadas a relaciones laborales y seguridad en los puestos de trabajo (por ejemplo aplicación de leyes laborales en cuanto a las solicitudes de indemnizaciones por parte de los trabajadores afectados); asuntos de seguridad y salubridad en la institución (por ejemplo las infracciones de las

normas laborales de seguridad e higiene), todo tipo de discriminación entre el personal también pueden ocasionar pérdidas financieras para las instituciones bancarias.

Procesos internos: son posibles pérdidas financieras relacionadas con el diseño inadecuado de las políticas y procedimientos inadecuados o inexistentes, o la planeación de los procesos críticos que pueden provocar deficiencias en las operaciones y servicios bancarios o bien la suspensión de los mismos. Tales casos pueden ser los riesgos ligados a las fallas en los modelos utilizados, los errores en los sistemas contables, errores en las transacciones, errores en los reportes, la inadecuada compensación o liquidación, así como el incumplimiento de plazos e insuficiencia de recursos para el volumen de transacciones. También está presente la inadecuada evaluación de los contratos o los productos financieros complejos, entre otros.

Sistemas: comprenden la posibilidad de pérdidas financieras producto del uso inadecuado de los sistemas de información y tecnologías, que pueden perturbar el desarrollo de las operaciones y servicios bancarios, atentando contra la confidencialidad, integridad, disponibilidad y oportunidad de información. Los siguientes eventos son parte de este riesgo: inadecuada inversión en tecnología o sistemas no compatibles o mal integrados, los errores de programación, las fallas en hardware, fallas de telecomunicación, errores de ingreso de los datos, inadecuada utilización de información confidencial, así como también la falta de seguridad tecnológica. Otros riesgos incluyen la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

Riesgos Externos: este grupo de riesgo está asociado con riesgos físicos que son ajenos al control de la empresa que pueden fuertemente alterar las actividades normales, perjudicando al mismo tiempo a los procesos internos, personas y sistemas de las instituciones financieras. Tal es el ejemplo de la ocurrencia de los actos de la naturaleza como los desastres naturales, incendios, terremotos, inundaciones. Los actos provocados por el hombre como el vandalismo, guerra y/o terrorismo también se consideran parte de este grupo de riesgos. Entre otros factores influyentes que ocasionan los terceros están los riesgos que implican las contingencias legales, las

fallas en los servicios de energía eléctrica, fallas de los terceros en el cumplimiento de los contratos de servicios, etc.

2.4 La importancia de gestión de riesgo operacional en la banca.

Durante los últimos años la administración y la mitigación del riesgo han tomado una especial importancia en el ámbito financiero internacional, donde las entidades financieras han venido realizando considerables esfuerzos por avanzar de manera decidida en materia de gestión del riesgo, principalmente enfocados hacia la medición e identificación de los riesgos más comunes, tales como el de mercado y el de crédito. No obstante, la creciente complejidad de los mercados y la mayor diversificación de los productos y servicios financieros, han generado paulatinamente el proceso de concientización en la industria financiera sobre la necesidad de profundizar en los temas del riesgo operacional, su prevención y mitigación.

Numerosos factores externos y el propio dinamismo del sector financiero afectan a la gestión operativa de las entidades de crédito y a sus resultados. Los procesos de fusión e integración, así como su internacionalización, dentro de mercados cada vez más globalizados, la incorporación de nuevas tecnologías (TIC) de las entidades de las que son cada día más dependientes, los contratos de outsourcing, de tercerización o externalización de las operaciones, promovidos por el ahorro de costos e inversiones, etc.; están transformando la cultura interna y la estructura operativa de las entidades de crédito. La dinámica de la competencia a nivel nacional e internacional, alentada desde los órganos reguladores, a fin de mejorar la eficacia de las entidades, propicia nuevas estrategias y el desarrollo de la innovación no solo en productos y servicios, también en canales de distribución, en procesos operativos, y en estilos y modelos de gestión empresarial[3].

Otro factor de peso, como las pérdidas operacionales millonarias por fraudes y otros eventos de riesgo operacional han sido hechos impulsadores de este proceso de concientización en torno, por una parte, a la necesidad de una administración efectiva

[3] JOSÉ IGNACIO LLAGUNO MUSONS *Gestión del riesgo operativo en las entidades de crédito: un camino sin retorno. Cuadernos de Gestión* Vol. 5. N.º 1 (Año 2005), pp. 53-77 ISSN: 1131

del riesgo operacional en las instituciones bancarias, y por otra parte, a una mejor supervisión de las actividades financieras de las entidades supervisoras de cada país.

El estudio del Banco Mundial sobre las fuentes de inestabilidad financiera en 29 países, donde se menciona que entre los factores endógenos que incidieron sobre crisis financieras se destacan en el primer y segundo lugar la supervisión insuficiente y la administración deficiente, respectivamente, seguidos por la inestabilidad política, préstamos relacionados y fraudes.

En el recuadro a continuación se puede apreciar la magnitud financiera de las pérdidas que ocasionaron algunos eventos históricos a nivel internacional:

Fuente de Riesgo	Entidad	Pérdidas	Suceso
Fraude Interno	BARINGS BANK	US$ 1.3 bill.	Nick Leeson, corredor de derivados, acumuló pérdidas no reportadas por 2 años. El banco se declaró en quiebra.
	DAIWA BANK Ltd	US$ 1.2 bill.	Toshihide Igushi, corredor de bonos, escondió pérdidas durante 11 años en una filial de USA. El banco fue multado por US$340.0 millones y se declaró en quiebra.
	National Westminster BANK (NatWest)	US$ 127 mill.	Kyriacos Papouis, corredor del mercado no organizado de swaptions, manipuló los precios de las operaciones para cubrir pérdidas. Daños reputacionales, el banco fue absorbido por Royal Bank of Scotland.
	Allied British BANK	US$ 750 mill.	John Rusnack, corredor del mercado de divisas, escondió pérdidas en operaciones sobre tasa de cambio Yen/USD en una subsidiaria de Baltimore USA, durante 3 años. Sistemáticamente falsificó registros bancarios y documentos, evadiendo los débiles controles existentes en la tesorería en la filial y casa matriz. Daños en la reputación del banco.
	CITIGROUP (Caso WorldCom)	US$ 2.6 bill.	Bernard Ebbers, presidente de WorldCom, realizó una serie de fraudes contables que llevaron a la quiebra de la compañía. El grupo Citigroup tuvo que llegar a un acuerdo extrajudicial con los accionistas a los que pagó esta suma de dinero a cambio de que retiraran la demanda colectiva que habían realizado, por considerar que el banco estuvo involucrado en el fraude al recomendar títulos de WorldCom a sabiendas de su frágil situación financiera.
	Société Générale	US$ 7.0 bill.	El mayor fraude llevado por un solo operador:

			malversación por parte de un empleado del banco que trabajaba en la división financiera y de inversiones de este banco y se dedicaba a la cobertura de futuros sobre índices bursátiles europeos.
Fraude Externo	Republic New York Corporation	US$ 606 mill.	Fraude cometido por el cliente privado de libertad
Prácticas de empleo y seguridad en el trabajo	Merrill Lynch	US$ 250 mill.	Resolución jurídica respecto a la discriminación de genero
Clientes, productos y prácticas empresariales	Household International	US$ 484 mill.	Prácticas abusivas de préstamos
	Providian Financial Corporation	US$ 405 mill.	Inadecuadas prácticas de ventas y facturación
Daños a los bienes físicos	Bank of New York	US$ 140 mill	Daños a instalaciones por los ataques terroristas del 11 de Septiembre
Interrupción de negocio y fallas de sistemas	Solomon Brothers	US$ 303 mill.	Cambio en la tecnología informática como resultado los “saldos sin conciliar”
Ejecución, entrega y gestión de procesos	Bank of America	US$ 225 mill.	Fallas en sistemas de integración provocan fallas en procesamiento de transacciones
	Wells Fargo Bank	US$ 150 mill.	Fallas en sistemas de integración provocan fallas en procesamiento de transacciones

A nivel local, lo que puede documentarse en materia de riesgos operativos son las multas aplicadas por la SIBOIF a las entidades que supervisa, las cuales se resumen a continuación:

- ✓ Por los incumplimientos derivados de los resultados de inspección In Situ (C$4.0 millones de córdobas)
- ✓ Por el incumplimiento de envío de información solicitada por el Superintendente en el plazo establecido para dicha remisión y entrega de informaciones fuera de fechas establecidas en el calendario oficial (C$0.7 millones de córdobas)
- ✓ Por el incumplimiento a instrucciones del Superintendente (C$0.2 millones de córdobas)
- ✓ Por el incumplimiento al Arto. 56 de la Ley 561, Ley General de Bancos, Instituciones Financieras No Bancarias y Grupos Financieros respecto al límite de concentración de crédito con partes relacionadas (0.2 millones de córdobas)

- ✓ Por el incumplimiento a la Norma sobre Gestión de Riesgo crediticio y la Norma sobre Contratación de Proveedores de Servicios (C$0.5 millones de córdobas)
- ✓ Por el incumplimiento en el establecimiento de las obligaciones recíprocas en los instrumentos contractuales de crédito (C$0.2 millones de córdobas)
- ✓ Otros incumplimientos.

Dichas multas sumaron la cantidad de C$6.0 millones de córdobas durante el período 2007-2009, que podría haberse evitado si las instituciones financieras implicadas cumpliesen con las disposiciones legales en su totalidad[4].

2.5 Gestión del riesgo operacional.

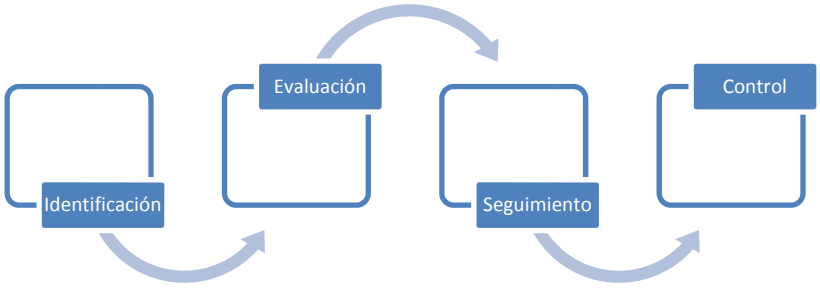
Como cualquier proceso administrativo, la gestión del riesgo operacional en un banco forma parte de todo un sistema organizativo que envuelve las políticas, procedimientos y estructuras específicas para lograr una gestión adecuada. Dicho sistema está construido en función de complejidad de las operaciones, cuyo funcionamiento se rige por los lineamientos emitidos y aprobados, cumpliendo las normas legales y de funcionamiento operativo.

Previo a mencionar las etapas de este proceso, cabe señalar que antes de entrar al proceso de gestión de este riesgo se debe empezar con una concientización a la alta gerencia sobre los beneficios y la necesidad de implantar todo este sistema. Dentro de las razones de peso pueden ser las presiones regulatorias internacionales e internas del país, la necesidad de obtener información de gestión sobre las causas y consecuencias del riesgo operacional, la comprensión del impacto de dicho riesgo, el poder asignar capital según el riesgo asumido, la necesidad de obtener más información que permita mejorar las decisiones sobre la mitigación del riesgo operacional, entre otras.

Al igual que en el caso de otros tipos de riesgo, el proceso de gestión del riesgo operacional se compone de varias etapas y su éxito depende de la consistencia y

[4] El detalle de multas impuestas por la SIBOIF para distintas instituciones financieras durante el período 2007-2009 se puede apreciar en el ANEXO No.1 del presente trabajo.

continuidad del mismo. Las etapas de este proceso se presentan en una cadena de acciones, iniciándose con la identificación de los riesgos operacionales, seguido con su evaluación y seguimiento para un posterior control o mitigación, siendo ésta última etapa la razón de todo el proceso, sin menosprecio de la importancia de cada una de las etapas:



En la etapa de *identificación* se toman en cuenta la procedencia del riesgo, tanto sus factores internos, como externos que afectan el logro de los objetivos institucionales. Se analiza la estructura de la entidad y la naturaleza de sus actividades, se determinan los cambios en el sector y avances tecnológicos, se revisan los procesos y políticas internas, etc.

En la etapa de *evaluación*, una vez identificados los riesgos operacionales, se deciden si se utilizan los procedimientos apropiados de control y/o mitigación. En este momento es cuando el banco decide si asumir el riesgo o administrarlo, dependiendo de la estrategia y el apetito al riesgo institucional. En el caso de los riesgos que no se pueden controlar se decide si se aceptan, reduce el nivel de actividad del negocio expuesta o se retira de esta actividad por completo.

El proceso de evaluación esta compaginado con la medición. Las entidades financieras deben estimar el riesgo inherente en todas sus actividades, productos, áreas particulares o conjuntos de actividades o portafolios, utilizando las técnicas cuantitativas para estimar el potencial de pérdidas (teniendo los datos históricos de por lo menos cinco años de actividades sin interrupción [5]), o técnicas cualitativas,

[5]El párrafo 672 del documento *"Convergencia Internacional de Medidas y Normas de Capital", BCBS, año 2004*, establece que las estimaciones del riesgo operativo generadas internamente en el banco y utilizadas a efectos de capital regulador deberán basarse en un periodo mínimo de cinco años de observación de datos internos de pérdida, ya se empleen directamente para estimar la pérdida o para

evaluando la probabilidad de ocurrencia e impacto en caso de materializarse el evento de riesgo; o bien, combinando ambos métodos para este fin.

Entre las herramientas para identificar y evaluar los eventos del riesgo operacional se puede destacar el proceso interno de auto-evaluación referido al uso de listas de control o de grupos de trabajo para identificar las fortalezas y debilidades del entorno del riesgo operacional. Para lograr la identificación de los riesgos operacionales, se debe partir del levantamiento y documentación de todos los procesos y procedimientos de la entidad financiera, teniendo claridad sobre los objetivos de cada proceso.

También, para este propósito se utiliza el mapeo de riesgos, donde se agrupan los eventos de las diferentes unidades del negocio, funciones organizativas y procesos por el tipo de riesgo correspondiente. Así mismo, se utilizan los indicadores de riesgo bajo los siguientes parámetros: número de operaciones fallidas, rotación del personal, frecuencia y gravedad de errores, etc.

Una vez identificados y evaluados los riesgos, a éstos se le da el *seguimiento o monitoreo*. La regularidad de este proceso permite detectar y corregir rápidamente las deficiencias en las políticas, procesos y procedimientos de gestión de riesgo operacional, detectando temprano los cambios materiales en el perfil de riesgo, así como la aparición de nuevos riesgos. El seguimiento se efectúa periódicamente, asegurando que las acciones implementadas están funcionando de forma oportuna y eficiente, informando o reportando sobre sus resultados a los niveles de alta gerencia, comité de riesgos o Junta Directiva.

Finalmente, la etapa de *control* se caracteriza por las medidas para mitigar el riesgo inherente con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que dicho riesgo se materialice. En esta etapa se establecen los procesos y procedimientos de control, un sistema adecuado que asegure el cumplimiento de las políticas establecidas, se reexaminan y se reajustan los procesos, procedimientos internos y tecnologías informáticas.

---

validar dicha estimación. Cuando el banco desee utilizar por vez primera los AMA, se aceptará un periodo histórico de observación de datos de tres años.

Una práctica efectiva de mitigar los eventuales daños para una entidad financiera es contar con una política de seguros efectiva que permite que el costo de posibles pérdidas se traslade a las compañías de seguros[6].

Otro tema de gran importancia en la etapa de control es la implementación y mantenimiento de un proceso para administrar la continuidad del negocio, el cual puede incluir los siguientes elementos: plan de prevención y atención de emergencias, plan de administración de crisis o el plan de contingencia y capacidad de retorno a la operación normal. Dichos planes están acorde al tamaño y complejidad de las operaciones de la entidad financiera y se actualizan periódicamente, así como se ponen en práctica a través de simulaciones dirigidas para comprobar su efectividad.

Otro elemento relevante, sin el cual no se podría lograr el éxito en la gestión del riesgo operacional en ninguna empresa ni organización, es el potencial del recurso humano y su disposición en trabajar alrededor del tema; las constantes capacitaciones del personal, las actualizaciones en las metodologías, procesos y sistemas informáticos garantizan una administración de riesgo operacional efectiva.

La implementación de una adecuada gestión del riesgo operacional para una entidad financiera implica la obtención de una serie de beneficios, entre ellos se pueden destacar los siguientes: la inclusión de la gestión de riesgos dentro de la planificación estratégica; reducción esperada de las pérdidas operacionales; una mejora de la imagen ante los inversionistas, accionistas, reguladores y clientes; la posibilidad de remunerar a ejecutivos sobre la base de riesgos, el fomento de la cultura y responsabilidad hacia el riesgo y la asignación de capital según el riesgo asumido.

[6] Los riesgos tradicionalmente asegurados se asocian a activos físicos, personal o tecnología. No obstante, a pesar de que no todos los riesgos son asegurables, su contratación genera un valor adicional para los accionistas a través de la estabilidad de los flujos de caja, prevención de catástrofes financieras, mayor supervisión y control, así como la gestión del riesgo a menor costo.

3 Marco Regulatorio base del Riesgo Operacional: Nuevo Acuerdo de Capital (Basilea II).

Generalidades

Basilea II es el Nuevo Acuerdo de Capital[7] que establece lineamientos generales para la banca mundial, los cuales pueden o no ser implementados por los reguladores de cada uno de los países. Dicho acuerdo fue propuesto por el Comité de Supervisión Bancaria de Basilea[8] con el fin de establecer un nuevo esquema de medición de los riesgos, incluyendo el riesgo operacional, que asumía la industria bancaria a nivel mundial, en el medio de un proceso de desarrollo, sofisticación tecnológica y globalización de los servicios financieros.

El aspecto nuevo de la Basilea II, el documento de la cual fue presentado por primera vez en el mes de junio de 1999 y cuya versión final fue publicada en el mes de junio de 2004, en comparación con el enfoque de la Basilea I del 1988[9], es considerar la gestión del riesgo operacional como una práctica integral comparable a la gestión de otros riesgos, tales como el riesgo crediticio y de mercado; además la principal novedad de Basilea II es la exigencia de capital regulatorio para afrontar dicho riesgo.

Basilea II se compone de tres pilares y en cada uno de ellos se toma en cuenta el riesgo operacional: el pilar 1 (requisitos mínimos de capital) al determinar los recursos propios, el pilar 2 (proceso de revisión de supervisión) al verificar que el capital calculado es apropiado y está bajo parámetros del perfil de riesgos de la entidad financiera, y el pilar 3 (disciplina del mercado) exigiendo que se revele la información relativa a la carga de capital y método aplicado para calcularlo.

---

[7] El nombre completo del documento en ingles es *"Internacional Convergence of Capital Measurement and Capital Standards: a Revised Framework"*.

[8] El Comité de Supervisión Bancaria de Basilea es una organización formada en el año 1974 por los gobernadores de los bancos centrales del Grupo de los Diez y está conformado por los representantes de la supervisión bancaria y bancos centrales de Alemania, Canadá, España (se agregó como miembro pleno en el año 2001), Estados Unidos, Francia, Italia, Japón, Luxemburgo, Países Bajos, Reino Unido, Suecia y Suiza. Su misión principal es establecer los estándares de supervisión relacionados con la solvencia de las entidades financieras. Aunque sus lineamientos y recomendaciones no tienen fuerza de ley, sin embargo son asumidas con carácter general en el ámbito internacional y son tomadas en cuenta en muchas legislaciones.

[9] El Acuerdo de Capitales de Basilea (BCBS, 1988), destinado a la cobertura del riesgo de crédito mediante capital y modificado en 1996 para incorporar el riesgo de mercado, quedando con el paso de tiempo obsoleto por no responder al nuevo entorno financiero y su escasa sensibilidad al riesgo.

En cuanto al cálculo del requerimiento mínimo de capital por riesgo operacional, Basilea II distingue tres métodos: el método de indicador básico, el método estándar y los métodos de medición avanzada. La utilización de cada uno de ellos está ligada al nivel ascendente de sofisticación de las actividades de la institución y su sensibilidad al riesgo. Además, el Comité de Basilea, establece que las Entidades de Intermediación Financiera (EIF) puedan utilizar cada método individualmente o una combinación de ellos para cada una de sus actividades. No obstante, para emplear los métodos estándar y de mediación avanzados, deben obtener autorización del supervisor, a partir del cumplimiento de criterios generales, cualitativos y cuantitativos.

Método del Indicador Básico (basic indicator approach o BIA)- las entidades que implementen este modelo deberán cubrir el riesgo operacional con un capital equivalente a un porcentaje fijo (factor alfa) del 15% del promedio del ingreso bruto de los últimos tres años[10] (si son negativos o cero, no se consideran).

Entre las ventajas de utilización del indicador básico se puede mencionar que es de fácil implementación y su aplicación es uniforme en toda la industria. Sin embargo, entre las inconvenientes de su empleo se destacan las siguientes: castiga innecesariamente los bancos con mayor margen financiero[11]; existen diferencias contables para definir los ingresos brutos; es insensible al riesgo y no incorpora riesgos de nuevos negocios; su aplicación tampoco incentiva una gestión adecuada del riesgo operacional, entre otros.

Método Estándar (standardized approach o SA)- bajo este método las actividades de los bancos se dividen en ocho líneas de negocio: finanzas corporativas, negociación y ventas, banca minorista, banca comercial, liquidación y pagos, servicios de agencia,

[10] Alfa=15% es el parámetro establecido por el Comité de Basilea que relaciona el capital exigido al conjunto del sector con el nivel del indicador en el conjunto del sector en base al estudio del grupo de trabajo *Risk Managment Group* denominado *"Loss data collection excercise for operational risk"*, en el cual se solicitaron los datos internos sobre el capital económico asignado por riesgo operacional a 89 entidades financieras en el año 2001 (la mitad de las cuales dieron la respuesta); que en conjunto con los datos recopilados en 1998-2000, arrojaron un promedio del 15%, aunque existía una notable dispersión entre el valor mínimo (1%) y máximo (40%).

[11] En este sentido el Nuevo Acuerdo de Capital, en su pilar 2 le otorga la facultad al supervisor de exigirle mayor capital a una institución en particular, precisamente porque el hecho de que una institución determinada tenga menos ingresos financieros que otra de igual tamaño, no significa que tiene menos riesgo operativo.

administración de activos e intermediación minorista. El requerimiento de capital de cada una de estas líneas de negocio se calcula multiplicando el ingreso bruto por un factor beta[12] que se asigna a cada una de las líneas, cuyos valores sugeridos por el Comité de Basilea son:

Factor Beta por líneas de negocio

▪ Finanzas Corporativas (18%)	▪ Pagos y Liquidación (18%)
▪ Negociación y Ventas (18%)	▪ Servicios de Agencia (15%)
▪ Banca Minorista (12%)	▪ Administración de Activos (12%)
▪ Banca Comercial (15%)	▪ Intermediación minorista (12%)

Fuente: Acuerdo de Capitales de Basilea

La exigencia total de capital es calculado como la media de tres años de la suma simple de las exigencias de capital regulador en cada una de la líneas de negocio de cada año[13].

Opcionalmente, existe un Método Estándar Alternativo, en el que los ingresos brutos de banca comercial y banca minorista se sustituyen por un 3.5% del total de préstamos y anticipos de cada una de las líneas de negocio.

Entre las ventajas del método estandarizado se puede destacar su fácil medición, una mayor precisión al desglosar el cálculo por línea de negocio y existencia de objetivos claros para las entidades financieras en relación a los cargos de capital. No obstante, este método de cálculo, al igual que anterior, sigue insensible al riesgo, así mismo la definición de ingresos brutos puede presentar diferencias contables y, aunque el cargo de capital puede ser menor que con la implementación del indicador básico, aún no incentiva a los bancos a gestionar el riesgo operacional eficientemente.

Métodos de Medición Avanzada (advanced measurement approach o AMA)- El Comité de Supervisión Bancaria de Basilea propone tres enfoques dentro de los AMA: los modelos de medición interna (internal measurement aproach o IMA); los modelos de distribución de pérdidas (loss distribution approach o LDA) y los cuadros de mando

[12] "Factor Beta" es una aproximación a la relación que existe en el conjunto del sector bancario ente el historial de pérdidas debido al riesgo operacional de cada línea de negocio y el nivel agregado de ingresos brutos generados por esa misma línea de negocio.
[13] Los requerimientos de capital negativos de cada año, producto de los ingresos negativos, en cualquiera de las líneas de negocio se compensa por los requerimientos positivos en otras líneas.

(scorecards). La utilización de estos métodos para el cálculo de capital por riesgo operacional está sujeta, según Basilea II, a la aprobación por parte de las autoridades de supervisión de cada país.

Entre los criterios generales que menciona Basilea II, tanto para aplicación del Método Estándar, como de la metodología AMA por parte del las entidades financieras, se destacan los siguientes: poseer un sistema de gestión de riesgo operacional sólido[14] y contar con los recursos para aplicar las metodologías de gestión en las principales líneas de negocio y en los ámbitos de control y auditoría interna; asegurar que el Directorio u órgano equivalente y la Alta Gerencia de la entidad financiera participen en la vigilancia del marco de gestión del riesgo operacional.

El método AMA, exige además que las instituciones financieras satisfagan un conjunto de criterios cualitativos y cuantitativos:

- *Criterios cualitativos:* contar con una unidad de gestión de riesgo operacional que se encargue del diseño y aplicación del marco de gestión del riesgo operacional; integrar el sistema de medición interna del riesgo operacional en los procesos habituales de gestión de riesgos de la institución financiera con el fin de que los resultados a ser arrojados por este sistema sean utilizados activamente en el proceso de seguimiento y control del perfil de riesgo operacional de la entidad financiera; informar periódicamente al Directorio y Alta Gerencia acerca de las exposiciones al riesgo operacional e historial de pérdidas a este riesgo con la finalidad de que Alta Gerencia este constantemente informada para poder adoptar las acciones necesarias; documentar el sistema de gestión de riesgo operacional y realizar las revisiones periódicas del proceso de gestión y sistemas de medición del riesgo operacional a través de las auditorías externas y/o internas.
- *Criterios cuantitativos:* El Comité de Supervisión Bancaria de Basilea no especifica supuestos sobre las distribuciones de probabilidad, pero establece

[14] Independientemente del método utilizado, el banco debe demostrar a su autoridad supervisora que su estimación de riesgo operacional satisface un criterio de solidez comparable al exigido en el método de tratamiento del riesgo de crédito basado en calificaciones internas (es decir, comparable a un período de mantenimiento de un año con un intervalo de confianza del 99.9 por ciento).

que el procedimiento para desarrollar el modelo de riesgo operacional debe ser riguroso, considerando datos externos, datos internos y análisis de escenarios, y entidad financiera debe demostrar que identifica los eventos de pérdidas ubicados en las colas de la distribución de probabilidad[15]. Estos modelos deben basarse en cinco años de información histórica[16].

Entre otros *criterios detallados* que complementan las exigencias para la utilización de los modelos AMA definidos en Basilea II se especifican los tipos de eventos de pérdida que se definen en el Anexo 7 del documento[17], agrupándose en una matriz de acuerdo a siete categorías de tipos de eventos (fraude interno; fraude externo; relaciones laborales y seguridad en el puesto de trabajo; clientes, productos y prácticas empresariales; daños a activos materiales e incidencia en el negocio y fallos en los sistemas), sus definiciones explicitas, categorización más detallada con sus ejemplos de actividades respectivamente. De tal manera que todo el sistema interno para el cálculo del riesgo operacional debe ser acorde a la definición del riesgo operacional establecida por el Comité de Supervisión Bancaria de Basilea[18] y a los tipos de eventos definidos en el Anexo 7. Así mismo, debe llevarse de acuerdo a las líneas de negocio establecidas en el Anexo 6 del mismo documento [19] , siguiendo los principios correspondientes. Cabe señalar que esta esquematización de agrupación de recopilación de pérdidas es sugerida por el Comité de Basilea para efectos de facilitar la supervisión bancaria, sin embargo, el banco puede decidir en qué medida desea aplicar esta clasificación de categorías dentro de su sistema de medición interna del riesgo operacional, siempre y cuando cumpla con las exigencias de su órgano regulador.

[15] Son los eventos de escasa probabilidad de ocurrencia pero de alto impacto monetario.
[16] Cuando se utilizan por primera vez, pueden basarse en tres años, incluyendo el año corriente de inicio.
[17] La información contenida en el Anexo 7 de la Basilea se puede visualizar en el ANEXO No.2 del presente trabajo.
[18] "El riesgo operativo se define como el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de la reputación"- párrafo 644 de la definición de riesgo operativo, Basilea II.
[19] La información contenida en el Anexo 6 de la Basilea se puede visualizar en el ANEXO No.3 del presente trabajo.

A diferencia del método de indicador básico y método estándar, las metodologías AMA son más sensibles al riesgo, pero a la vez son más costosas y complejas y su principal obstáculo para la implementación es la disponibilidad de una base de datos interna de pérdidas con las que aproximar las variables a utilizar, así como de una base externa, para poder combinar ambas informaciones.

2.7 Marco legal de la administración de riesgo operacional en Nicaragua.

Generalidades

Como se había mencionado en los acápites anteriores, el riesgo operacional involucra tanto el desenvolvimiento interno de las operaciones de una institución financiera, como las relaciones con los terceros y los factores externos que pueden ser causantes de la presencia de dicho riesgo. La construcción de un sistema de control preventivo de estas circunstancias por parte de las entidades financieras coadyuva a determinar el riesgo operacional en sus etapas tempranas o minimizar los daños efectivamente.

La contraparte externa de este proceso es precisamente el órgano rector del sistema financiero de cada país, dentro de las facultades del cual esta regular el buen funcionamiento del sistema financiero. Esta función de regulación no hace que los riesgos, entre ellos el operacional, se desaparezcan, no obstante, procura que se administren adecuadamente.

Los bancos no son unas islas dentro de la actividad económica de un país, sino que forman parte integral de las economías: estimulan el ahorro y facilitan la inversión, sirven de mecanismo de transmisión de política monetaria, su infraestructura ayuda al sistema de pagos del país. Otro factor de suma importancia para ser supervisados es el hecho de que por lo general más del noventa por ciento de sus activos son financiados con los depósitos del público, por lo tanto éstos últimos deben estar bien administrados y asegurados, procurando la solidez del sistema bancario.

De acuerdo a uno de los principios básicos en la gestión y supervisión del riesgo operacional que recomienda el Comité de Basilea en su documento “Sound practices

for the management and the supervisión of operational risk"[20], el papel de los supervisores en esta materia es exigir a los bancos que tengan un marco de gestión del riesgo operacional implantado y deben revisarlo.

La Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF), órgano supervisor y fiscalizador de las instituciones financieras bancarias y de otras instituciones financieras, entre las facultades concebidas según su ley creadora, y atribuciones del Consejo Directivo se establece la potestad de dictar normas generales para evitar o corregir irregularidades o faltas en las operaciones de las Instituciones Financieras que, a juicio del Consejo Directivo, pudieran poner en peligro los intereses de los depositantes, la estabilidad de alguna Institución o la solidez del Sistema Financiero.

Por su parte, la Ley 561, Ley General de Bancos, Instituciones Financieras No Bancarias y Grupos Financieros en su artículo 38, numeral 4) estipula que las juntas directivas de los bancos tienen entre sus responsabilidades el "Velar porque se implementen e instruir para que se mantengan en adecuado funcionamiento y ejecución, las políticas, sistemas y procesos que sean necesarios para una correcta administración, evaluación y control de los riesgos inherentes al negocio"

El proceso de regulación por parte de la SIBOIF de los temas relacionados con el riesgo operacional fue paulatino, iniciándose con la aprobación de la normativa sobre la Administración Integral de Riesgos en el año 2006, posteriormente en este mismo año fue emitida la normativa sobre Outsourcing. Luego en el año 2007 se aprobó la Norma de Gestión de Riesgo Tecnológico, y finalmente a inicios del año 2010 se aprobó la norma específica sobre Gestión de Riesgo Operacional. Adicionalmente a lo anterior, se ha normado de forma específica el riesgo operacional relacionado al tema de prevención de lavado de activos y financiamiento al terrorismo.

[20] "Los principios básicos constituyen un marco voluntario de normas mínimas para las prácticas de supervisiones sólidas; las autoridades nacionales tienen la libertad de adoptar las medidas complementarias que crean necesarias para alcanzar la supervisión efectiva en sus jurisdicciones"- nota aclaratoria del párrafo 5 del documento *"Principios Básicos para una Supervisión Efectiva", BCBS, Octubre 2006.*

Norma sobre la Administración Integral de Riesgos

La presente norma fue aprobada por la SIBOIF el 30 de mayo del 2006 y establece básicamente las disposiciones mínimas sobre la administración integral para distintos riesgos, incluyendo el operacional, obligando a las instituciones financieras que dichos riesgos se identifiquen, se midan, se limiten, se controlen, así como se informe sobre ellos a la SIBIOF, con el fin de mitigar o eliminar el posible impacto negativo de dichos riesgos.

En la Norma sobre Administración Integral de Riesgo, el riesgo operacional está definido como "el riesgo de pérdida debido a la inadecuación o fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos y comprende, entre otros, el riesgo tecnológico, el riesgo de lavado de dinero y de financiamiento al terrorismo[21], así como el riesgo legal".

Dentro de los aspectos generales de la administración del riesgo operacional la presente norma estipula las funciones mínimas que corresponden desarrollar al comité de riesgos[22] y a la unidad de administración integral de riesgos:

- ✓ *Comité de Riesgos:*
  - Evaluar e informar por lo menos trimestralmente, las consecuencias sobre el negocio la materialización de los riesgos identificados e informar los resultados a los responsables de las unidades implicadas, a fin de que se evalúen las diferentes medidas de control de dichos riesgos;
  - Establecer los niveles de tolerancia para cada tipo de riesgo identificado, definiendo sus causas, orígenes o factores de riesgo;
- ✓ *Unidad de Administración Integral de Riesgos (UAIR):*

[21] Dicha normativa establece que la gestión del riesgo de lavado de dinero y de financiamiento al terrorismo se realizará de conformidad con la normativa de la materia.
[22] El comité de riesgo, de acuerdo a la misma norma, se conforma de miembros propietarios de la junta directiva con participación (con voz pero sin voto) de los siguientes invitados: el ejecutivo principal o gerente general, el responsable de la unidad de administración integral de riesgos, el auditor interno de la institución financiera y los responsables de las distintas unidades de negocios y de soporte operativo involucrados en la toma de riesgos (en este caso de riesgo operacional).

- Identificar y documentar los procesos que describen el quehacer de cada unidad de la institución y de sus riesgos operacionales;
- Establecer los niveles de tolerancia para cada tipo de riesgo identificado, definiendo sus causas, orígenes o factores de riesgo;
- Crear la cultura de riesgo operacional a través de la divulgación de documentos informativos;
- Desarrollar el método de almacenamiento de las pérdidas operacionales;
- Implementar la metodología para la administración del riesgo operacional, en el cual se conozcan y cuantifiquen los principales riesgos operacionales de la institucional, se enfoquen los esfuerzos de control para su mitigación en las áreas de mayor sensibilidad, y se mejoren los distintos procesos de toma de decisiones;
- Recibir la información correspondiente a los eventos de pérdidas por riesgo operacional, y determinar: área que genera el riesgo, área que registra la pérdida, causas, medidas correctivas, categoría;
- Monitorear el cumplimiento de las recomendaciones de Auditoría Interna y Externa;
- Entre otras.

Para el desempeño de las funciones por parte de la UAIR, las instituciones deberán establecer mecanismos que aseguren un adecuado flujo, calidad y oportunidad de la información entre esta unidad y el resto de órganos al interior de la institución.

Además de abordar los aspectos generales de la administración del riesgo operacional, la normativa sobre la administración integral de riesgos aborda sobre las funciones de la UAIR en cuanto al riesgo tecnológico, evaluando las circunstancias que pudieran influir en las operaciones ordinarias, y el riesgo legal, ambos forman parte del riesgo operacional, como lo señala la misma norma:

Funciones de la UAIR sobre el Riesgo Tecnológico	Funciones de la UAIR sobre el Riesgo Legal
•Evaluar la vulnerabilidad en el hardware, software, seguridad, recuperación de información y redes, por errores de procesamiento u operativos, faltas en procedimientos, capacidadea inadecuadas, insuficiencia de los controles instalados, entre otros; •Considerar en la implementación de controles internos, respecto del hardware, software, seguridad, recuperación de información y redes de la institución, al menos, los siguientes: •proponer políticas y desarrollar procedimientos que aseguren en todo momento el nivel de calidad del servicio, la seguridad, disponibilidad e integridad de la información •asegurar que para cada operación o actividad realizada por los usuarios existan registros de auditoría en las bases de datos y software utilizados •implementar mecanismos que midan y aseguren niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución y desempeño de las operaciones y servicios realizados.	•Proponer políticas y desarrollar procedimientos para que en forma previa a la celebración de actos jurídicos, se analice la validez jurídica y procure la adecuada instrumentalizsación legal de estos, incluyendo la formalización de las garantías a favor de la instititución; •Estimar el monto de pérdidas potenciales derivado de resoluciones judiciales o administrativas adversas, así como la posible aplicación de sanciones, en relación con las operaciones llevadas acabo; •Analisar los actos que se realice la institución cuando se rijanpor un sistemas jurídico distinto al nacional, y evaluar las diferencias existentes entre el sistema de que se trate y el nacional, incluyendo lo relativo al procedimiento judicial; •Dar a conocer a sus directivos y empleados, las disposiciones legales y administrativas aplicables a las operaciones; •Mantener una base de datos histórica sobre las resoluciones judiciales y administrativas, sus causas y costos.

Dentro de otras funciones que se le otorgan a la UAIR en función de las operaciones bancarias con clientes a través de internet, cajeros automáticos, banca telefónica, sucursales, que implican el manejo del riesgo operacional, se destacan los siguientes:

- Establecer medidas y controles de seguridad en la generación, transmisión y recepción de las claves de identificación y acceso para los usuarios;
- Contar con esquemas de control y políticas de operación, autorización y acceso a los sistemas, bases de datos y aplicaciones implementadas para la realización de operaciones bancarias a través de cualquier medio tecnológico;
- Incorporar los medios adecuados para respaldar y, en su caso, recuperas, la información que se genere respecto de las operaciones bancarias que se realicen a través de cualquier medio tecnológico;
- Diseñar planes de contingencia y recuperación, a fin de asegurar la capacidad y continuidad de los sistemas implementados para la celebración de operaciones bancarias;
- Establecer mecanismos para la identificación y resolución de aquellos actos o eventos que pueden generar a la institución, riesgos derivados de los hechos irregulares a través de medios tecnológicos, el uso inadecuado por

parte de los usuarios de los canales de distribución y contingencias generadas en los sistemas relacionados con los servicios bancarios prestados, entre otros.

Cabe señalar que las UAIRs, para dar cumplimiento a las funciones descritas anteriormente, podrán auxiliarse en las áreas que se estimen convenientes, siempre y cuando con ello no se causen conflictos de interés dentro de la estructura organizacional de la institución bancaria.

Norma sobre la Contratación de Proveedores de Servicios para la Realización de Operaciones o Servicios a Favor de las Instituciones Financieras

Presente norma de la SIBOIF hace referencia a los requisitos mínimos que debe cumplir una institución financiera en cuanto a la contratación de terceros proveedores de servicios, siendo necesario para las instituciones financieras al menos: evaluar los riesgos asociados a los acuerdos de contratación existentes y propuestos; desarrollar parámetros que ayuden a determinar la materialidad de dichos riesgos; implementar un programa de administración y monitoreo de los riesgos en función de materialidad de la operación contratada y asegurar que las autoridades del banco reciban la información necesaria y pertinente.

Esta norma otorga las responsabilidades a la junta directiva para aprobar y/o revaluar las políticas de contratación a terceros, parámetros de materialidad, programas de gestión y administración de riesgos relacionados, así mismo, se establecen las responsabilidades de la elaboración e implementación de estas políticas a la instancia de administración integral de riesgos.

Las políticas de contratación a terceros deben exponer la filosofía de los riesgos como base para la toma de decisiones y parámetros para administrar los riesgos, deben evaluarse la materialidad de las contrataciones, desarrollarse los planes de gestión y administración de riesgos, así como deben especificar la autoridad de aprobación a delegarse, los funcionarios a quienes se delega y los factores a ser utilizados para los

límites de contratación (el tipo de actividad a contratarse, la experiencia del proveedor del servicio y el porcentaje del servicio a contratarse).

Entre los aspectos a considerar para establecer la materialidad de una operación se mencionan los siguientes cuantitativos y cualitativos:

- ✓ El impacto financiero, reputacional y operacional en la institución financiera en caso que el proveedor de servicios no realice la operación encomendada de manera adecuada;
- ✓ Pérdidas potenciales para los clientes de la institución financiera y sus contrapartes en caso de fallas atribuibles al proveedor del servicio;
- ✓ Costo y complejidad de la contratación;
- ✓ Posibles consecuencias legales;
- ✓ Marco regulatorio del proveedor;
- ✓ Interrelación de la operación contratada con el resto de operaciones de la institución financiera;
- ✓ Grado de dificultad y tiempo requerido para seleccionar un proveedor alterno si fuese necesario;
- ✓ Entre otros.

También la norma habla sobre las evaluaciones previas a la contratación del proveedor y los aspectos necesarios a ser analizados y determinados en el contrato. Dentro de éstos últimos se mencionan los siguientes: naturaleza y alcance del servicio a ser proveído, parámetros de cumplimiento, plazos y forma, requisitos de información, resolución de disputas, incumplimiento y terminación, propiedad y acceso, planes de contingencia, auditoría, subcontratación, precio, seguros, entre otros.

Otro elemento importante de esta norma es que estipula que el Superintendente con el fin de prevenir cualquier situación de riesgo podrá suspender, limitar o prohibir la contratación de cierto tipo de operaciones o servicios a terceros, tomando en consideración la materialidad del acuerdo de contratación y la protección del interés público en la intermediación financiera.

Norma sobre Gestión de Riesgo Tecnológico

Esta norma se aprobó con el fin de establecer los criterios mínimos de evaluación sobre la administración de los riesgos, la seguridad, la utilización y los controles aplicados a las Tecnologías de Información (hardware, software, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, servicios y organización de informática), con el fin de velar por la estabilidad y la eficiencia del sistema financiero.

La norma establece que para la gestión de las tecnologías de información y sus riesgos asociados se considerarán los siguientes criterios relacionados con la información: confidencialidad, confiabilidad, disponibilidad, efectividad, eficiencia, integridad y cumplimiento.

Así mismo, se establecen las responsabilidades de la junta directiva y alta gerencia en cuanto a velar por la existencia de un Gobierno de Tecnología de Información; aprobar los objetivos, lineamientos y políticas generales para administrar la seguridad y los riesgos de tecnología de la información; proveer los recursos necesarios para lograr el cumplimiento de estas políticas; aprobar los planes de TI; velar por la implementación de sistemas de información propios o adquiridos; asegurar por la disponibilidad, capacidad y el desempeño de los sistemas de información requeridos para la continuidad del negocio; velar por el uso responsable de los recursos de TI y administrar adecuadamente los riesgos de TI.

También se prevé la realización y actualización de una planeación de tecnologías de información por parte de las instituciones financieras, considerando como mínimo: la definición de soportes a los programas de inversión y la entrega de los servicios operacionales; definición del plan de infraestructura tecnológica; el cumplimiento de una política de adquisición y mantenimiento de la infraestructura tecnológica; el presupuesto de la inversión de TI; las estrategias de adquisición y requerimientos legales y regulatorios.

En términos generales, Norma sobre gestión de riesgo tecnológico obliga a las instituciones financieras a implementar los procedimientos internos que permiten

autoevaluarse e informar a la junta directiva, al menos una vez al año sobre los resultados de esta evaluación.

En cuanto a la adquisición, desarrollo e implementación de tecnologías de información, se establece que las instituciones deben definir sus propias políticas de aprobación de proyectos de TI; se determina la documentación necesaria a tener en caso de los nuevos proyectos; metodología para los sistemas internos que rija los procesos, análisis, diseño, desarrollo, implementación y mantenimiento de sistemas computarizados y tecnología; se exige a contar con estándares y convenciones de nomenclatura en sus códigos fuentes a fin de garantizar la continuidad operativa de los procesos de desarrollo y la capacidad de integración entre aplicaciones de software desarrollados.

De igual forma, la Norma sobre gestión de riesgo tecnológico estipula que se deben definir adecuados procedimientos de cambios a producción para proteger los programas de aplicación de cambios no autorizados. Así mismo, en el caso de situaciones donde se requiera llevar a cabo cambios de emergencia para resolver problemas del sistema y para posibilitar la continuidad de un procesamiento crítico, se establece que deben existir los procedimientos de emergencia que no comprometan la integridad de la institución.

Referente a la administración de tecnologías de información, la norma establece que las instituciones deben contar con las políticas y procedimientos documentados para asegurar que su plataforma tecnológica no sea usada para el resguardo, copia, distribución o uso de cualquier programa de aplicación, software de oficina, contenido multimedia o cualquier otro material en forma digital, cuyos derechos no hayan sido adquiridos por la institución financiera y cuyo uso no esté autorizado.

Entre otros aspectos de destaca que las instituciones financieras deben definir políticas y procedimientos para la adecuada instalación, mantenimiento y administración de software; administrar la base de datos, hardware, las redes y líneas de comunicación de misión crítica. Así mismo, las instituciones deben asegurarse que todas las tareas o procesos internos de TI sean debidamente documentado con el fin de lograr un entorno operativo que tenga un nivel adecuado de madurez.

Relativo a la administración de seguridad Norma sobre gestión de riesgo tecnológico refleja que las instituciones deben también establecer las políticas y procedimientos de seguridad de información referentes a: clasificación y protección de activos de información; seguridad del acceso a los sistemas de información; el uso adecuado de los equipos de computo; el uso de Internet y de correo electrónico. Así mismo, las instituciones deben definir una política de limitación y control de acceso a programas, bases de datos, servicios de redes y sistemas operativos; procedimientos para reducir los riesgos asociados al error humano, robo, fraude o mal uso de activos vinculados al riesgo de TI. De igual forma las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar protegidos contra los accesos no autorizados, daños e intrusiones, entre otros.

Por otra parte, la Norma sobre gestión de riesgo tecnológico prevé también los diferentes aspectos relacionados con administración de problemas, planeación de contingencia y estrategias de recuperación, entre los cuales se pueden destacar los siguientes:

- ✓ Debido al carácter complejo de la tecnología, deben existir mecanismos para administrar incidencias, problemas y errores, permitiendo la identificación, análisis, solución y documentación de errores;
- ✓ Las instituciones deben establecer procedimientos de respaldos de información regulares y periódicamente validados para asegurar que se resuma el procesamiento normal de la información en caso de interrupción de corto plazo y/o si hay necesidad de procesar o de reiniciar un proceso;
- ✓ El establecimiento de procedimientos de respaldo con frecuencia razonable en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento;
- ✓ Como parte de la planeación de continuidad del negocio las instituciones deben considerar la participación de tecnología de la información en sus planes de contingencia y recuperación de desastres;
- ✓ Las instituciones deben contar con cobertura de seguros para los principales equipos de cómputo y comunicaciones que permita mitigar al menos riesgos

provocados por incendio, accidentes, fenómenos naturales, huelgas, motines y robo.

Finalmente, en cuanto al uso de la metodología de administración integral de riesgo tecnológico a aprobarse la presente norma estipula que se deben considerarse los aspectos cualitativos y cuantitativos de análisis de riesgo:

Analisis Cuantitativo de Riesgo Tecnológico	Análisis Cualitativo de Riesgo Tecnológico
•La conformación de una base de datos histórica de eventos de pérdida o frustración de ganancia producto la materialización de riesgos tecnológicos. •La determinación de la frecuencia de ocurrencia de dichos eventos; •La determinación de su impactoo severidad; •La estimación y aprovisionamiento del valor en riesgo en base a información histórica razonable	•La categorización de los riesgos; •La determinación de los riesgos inherentes a cada proceso que involucre el uso de tecnología de la información,describiendo su composición en amenazas y/o vulnerabilidades, su probabilidad de ocurrencia e impacto; •La identificación de controles que mitiguen los riesgos identificados, su clasificación (detectivos, disuasivos, preventivos, y/o correctivos), su nivel de efectividad y cumplimiento; •La determinación del riesgo residual resultante de la aplicación de los controles a los riesgos; •La determinación de los niveles aceptables de riesgo; •La identificación y seguimiento a planes de mejora •La realización de matrices y/o mapas de riesgo o severidad

Norma sobre Gestión de Riesgo Operacional

Nicaragua es uno de los países de la región que cuenta con una norma específica sobre la gestión de riesgo operacional, la cual fue emitida por el Consejo Directivo de la Superintendencia de Bancos y de Otras Instituciones Financieras el reciente 22 de enero del año 2010.

A través de la misma, la SIBOIF determina los conceptos en materia del riesgo operacional referidos en la presente norma; establece las responsabilidades que deben tener las instituciones financieras en la gestión del riesgo operacional y define los lineamientos generales para esta gestión, con el fin de controlar o mitigar el posible impacto negativo del dicho riesgo; así como determina los criterios especiales a tomar en cuenta para mantener el control efectivo de los principales factores de riesgo operacional a los que pueden estar expuestas las instituciones financieras. Así mismo,

en el anexo adjunto estipula los elementos y principios básicos para la gestión efectiva de la continuidad del negocio.

El concepto del Riesgo Operacional determinado en la norma nacional es similar al concepto propuesto por el Comité de Basilea y expresa lo siguiente: “es el riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, las personas o los sistemas o por eventos externos. Esta definición incluye al riesgo legal y tecnológico, pero excluye el riesgo estratégico y reputacional”.

Dentro de las *Responsabilidades de Gestión* del riesgo operacional que se estipulan en la presente norma, se destacan los siguientes aspectos:

- ✓ Las instituciones financieras deben contar con un *sistema de gestión de riesgo operacional* que les permita identificar, medir, controlar, mitigar y monitorear su exposición a este tipo de riesgos en el desarrollo de sus negocios y operaciones. La implementación de este sistema debe estar agrupado por líneas de negocio de la institución.

  Debido a que cada institución tiene su propia estructura, naturaleza y complejidad de operaciones, se establece que las identidades financieras deben formalizar sus propios controles y procedimientos para la gestión del dicho riesgo.

- ✓ Se determinan las *responsabilidades de la junta directiva* en cuanto a la gestión del riesgo operacional, lo que cubre tanto la aprobación de los objetivos, lineamientos y políticas sobre el riesgo operacional al que está expuesta cada institución, como el cumplimiento de dichos objetivos, lineamientos y políticas aprobadas.
- ✓ Al igual como para otros tipos de riesgo, se establece que los objetivos, lineamientos y políticas del riesgo operacional deben estar claramente definidos en los *manuales de gestión* a ser aprobadas por la junta directiva que servirán como soporte funcional y operativo al proceso de gestión del riesgo operacional en cada institución financiera.

Estos manuales deben ser documentos técnicos que contengan, entre otros, los diagramas de flujo de información, modelos y metodologías para la evaluación del riesgo operacional, así como, los requerimientos de los sistemas de procesamiento de información y análisis de riesgos.

Las juntas directivas deberán aprobar, al menos, los siguientes manuales:

Manual de Políticas y Procedimientos	Manual de Organización y Descripción de Funciones	Manual de Control de Riesgo Operacional
•políticas y procedimientos para la identificación, medición, control, adecuación, seguimiento y administracuión del todos los riesgos •las acciones correctivas a ser implementadas y del seguimiento •sistemas preventivos para detectar los riesgos y los mecanismos de vigialncia •mecanismos de elaboración e intecambio de información, tanto interna, como externa •acciones previstas para la difusión de las actividades que corresponden a los deferentes niveles directivos y al personal sobre el control de sus tareas.	•detalle de la organización funcional de la institución •las funciones, cargos y responsabilidades de los funcionarios en todos sus niveles.	•la definición clara de riesgo operacional, estableciendo los principios para su identificación, evaluación, monitoreo, control y mitigación. •políticas para la administración del riesgo operacional •funciones y responsabilidades de la unidad responsable del control y analisis del riesgo operacional; así como, las unidades de negocio y de apoyo en la administración de dicho riesgo •descripción de metodología aplicada para la medición y evaluación del riesgo operacional •la forma y periodicidad de informar a la junta directiva y a la alta gerencia •el proceso para aprobación de propuestas de nuevas operaciones, productos y servicios, identificando los riesgos y las acciones a tomar para su control.

- ✓ *Unidad responsable de la gestión del riesgo (UAIR)*- se establece que estas unidades ya creadas por la Normativa de administración integral de riesgos en cada una de las entidades serán también las responsables del control y análisis del riesgo operacional y se regirán tanto por la presente normativa, como por la antes mencionada.

Los Lineamientos a seguir para gestionar el riesgo operacional como las generalidades mínimas en cuanto al establecimiento de los objetivos, políticas y procedimientos de este riesgo, se enfocan en nueve líneas de acción:

Primeramente se exige a las entidades financieras a identificar, por línea de negocio, los eventos de riesgo operacional agrupados por tipo y fallas, o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos, entre otros: fraude interno; fraude externo; prácticas laborales y seguridad del ambiente de trabajo; prácticas relacionadas con los clientes, los productos y el negocio; interrupción del negocio por fallas en la tecnología de información; y deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

El siguiente paso después de identificar los eventos generadores del riesgo operacional o las fallas y su incidencia institucional, se indica que la junta directiva y la alta gerencia deben decidir si aceptan el riesgo identificado, lo comparten, lo evitan o lo transfieren, reduciendo sus consecuencias y efectos en el desempeño de la entidad financiera. Para lo cual deben adoptar las siguientes acciones: revisar estrategias y políticas; actualizar o modificar procesos y procedimientos; implantar o modificar límites de riesgo; construir, incrementar o modificar controles; implantar planes de contingencia y de continuidad del negocio; revisar términos de pólizas de seguro contratadas; contratar servicios de outsourcing u otros.

Otro componente sustancial en el proceso de gestión es conformación de la base de datos, lo cual también incluye la norma de la SIBOIF, señalando que las instituciones financieras deben conformarla de manera centralizada que permita registrar, ordenar, clasificar y disponer de información sobre los eventos y factores de riesgo operacional, fallas o insuficiencias, clasificados por línea de negocio, determinando la frecuencia de los eventos y el efecto cuantitativo de pérdida producida. Dicha información sirve para estimaciones de las pérdidas esperadas e inesperadas atribuibles al riesgo operacional, la regulación de lo cual está abierta para una normativa futura específica para tal materia.

El lineamiento sobre la tecnología de información estipula que cada institución debe contar con TI que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna, segura y confiable; mitigar las interrupciones del negocio y lograr que la información, inclusive la de terceros, sea íntegra, confidencial y éste disponible para una apropiada toma de decisiones[23].

En cuanto a garantizar la suficiencia continua de la información, la norma sobre la gestión del Riesgo Operacional establece que las instituciones financieras deben contar con un sistema organizado de reportes que permite disponer de información suficiente y adecuada. Por lo cual los reportes deben contener al menos la siguiente información:

- ✓ Detalles de los eventos de riesgo operacional, agrupados por tipo de evento las fallas o insuficiencias que los originaron relacionados con los factores de riesgo operacional, clasificada por línea de negocio; con las pérdidas asignadas por cada evento;
- ✓ Informes de evaluación por partes de la auditoría interna con respecto del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operacional, los procesos y procedimientos establecidos por la institución;
- ✓ Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados. Los informes relacionados deben ser dirigidos a las áreas correspondientes de la institución, para que puedan ser

[23] En más detalle los aspectos relacionados con el riesgo tecnológico están contenidos en la norma específica señalada previamente.

analizados con la perspectiva de constante mejora en el desempeño de la administración del riesgo operacional, entre otros.

Por otra parte, la norma sobre Gestión de Riesgo Operacional establece que las instituciones deben asignar responsables que se encarguen de definir y autorizar de manera formal los accesos, cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos. Así mismo, estas autoridades responsables deben definir las políticas, procesos y procedimientos bajo las mejores prácticas aplicables[24] que garanticen en la ejecución de los criterios de control interno relativos a eficacia, eficiencia, y cumplimiento de éstos, alineados a los objetivos y actividades de la institución, los cuales deberán ser aprobados por la junta directiva.

Debido a que dentro de los factores externos del riesgo operacional están los riesgos relacionados con los terceros, la presente norma de la SIBOIF incorpora dentro de sus lineamientos la subcontratación de servicios (tercerización), destacando que la institución financiera debe proceder en estas situaciones conforme la normativa que regula la materia sobre contratación de proveedores de servicios, mencionada anteriormente.

El punto especial dentro de los lineamientos definidos por la Norma sobre la Gestión de Riesgo Operacional está relacionado con la gestión efectiva de la continuidad del negocio, la cual enmarca todas las operaciones de negocios de la institución financiera e incluye las políticas y procedimientos que deben asegurar el mantenimiento de las operaciones específicas o recuperarlas oportunamente en el caso de una interrupción ya sea a causa de los factores internos o externos. Esto con el fin de minimizar las consecuencias operacionales, financieras, legales, materiales, entre otras.

Entre los elementos establecidos para una efectiva gestión de la continuidad de negocio se destacan los siguientes:

- ✓ Análisis de impacto como punto inicial en la gestión, donde se identifiquen las operaciones y servicios críticos, dependencias internas y externas claves y

[24] Son los marcos de referencia de estándares internacionales que ayuden a monitorear y mejorar las actividades críticas, aumentando el valor del negocio, tales como las recomendaciones del Comité de Basilea, COSO, COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2, entre otros.

niveles apropiados de resistencia; se evalúe midiendo cuantitativamente y cualitativamente los riesgos e impactos potenciales de varios escenarios de interrupción en las operaciones de una institución financiera; con el fin de identificar los aspectos prioritarios para la recuperación, los requisitos de recursos para la recuperación, el personal esencial , etc.

- ✓ Estrategia de recuperación, donde se establecerán los objetivos de recuperación y prioridades basadas en el análisis de impacto previo, destacándose por ejemplo, los objetivos para el nivel de servicios que la institución procuraría prestar en caso de interrupción y la infraestructura necesaria para el restablecimiento total de las operaciones del negocio.
- ✓ Planes de continuidad del negocio en forma de una guía detallada para la implementación de la estrategia de mantenimiento y recuperación. En esta etapa se establecerán los roles y se delegarán las responsabilidades para el manejo de interrupciones operacionales y se proporcionarán las pautas claras con respecto a la sucesión de la autoridad en casos de interrupciones que perjudiquen al personal clave. También se establecerán de manera clara la autoridad para la toma de decisiones y las circunstancias o eventos que activen el plan de continuidad de negocios de la institución financiera, considerando la seguridad del personal en todo el proceso de implementación del dicho plan.

Entre las responsabilidades de la junta directiva y de la alta gerencia en relación específicamente a la continuidad del negocio se destaca que ellos deben crear y promover una cultura organizacional que tenga como prioridad la continuidad del negocio, siendo ésta un componente clave de la gestión integral de riesgos en la institución.

Entre las acciones particulares sobre la continuidad del negocio, se establece que el sistema interno de gestión creado permita que la junta directiva y alta gerencia sean informados sobre el grado de su implementación, notificaciones de incidentes, resultados de las pruebas y acciones relacionadas al fortalecimiento de la resistencia de la institución o habilidad para reanudar operaciones específicas. Así mismo, la gestión de la continuidad del negocio debe estar sujeta a revisión por los auditores,

tanto externos como internos, cuyos hallazgos deben ser puestos en conocimiento de la junta directiva y de alta gerencia.

En el caso de interrupciones mayores, las cuales presentan un riesgo sustancial a la continuidad de las operaciones del sistema financiero, éstas también deben estar incluidas dentro de los planes de continuidad del negocio de las instituciones. Debido a que las interrupciones mayores podrán variar en alcance y duración, al evaluar si su gestión de continuidad es o no suficiente para dar respuesta, las instituciones deben revisar la adecuación de sus mecanismos en las siguientes áreas:

- ✓ Tener el cuidado de que su sitio alterno se encuentre lo suficientemente alejado del lugar donde llevan a cabo sus operaciones;
- ✓ El sitio alterno debe contar con la información actualizada suficiente y los equipos y sistemas necesarios para minimizar los efectos de las interrupciones de los servicios críticos;
- ✓ En el caso de que el personal de la oficina no se encuentre disponible, el plan de continuidad de negocio debe incluir la forma en que la institución proveerá el personal adecuado en términos numéricos y de experiencia, para la reanudación de las operaciones y servicios críticos que sean consistentes con el objetivo de recuperación.

Así mismo, las instituciones financieras deben incluir en sus planes de continuidad los mecanismos de comunicación efectiva con las partes interesadas relevantes, tanto dentro, como fuera de la institución, en caso de las interrupciones mayores. Se deben identificar las personas responsables de comunicarse con el personal y demás partes externas; el personal responsable puede incluir alta gerencia, encargados de relaciones públicas, asesores legales y el personal responsable de continuidad del negocio de las instituciones. Dicho grupo de responsables debe estar en capacidad para comunicarse con personal ubicado en lugares remotos.

Los planes de continuidad del negocio deben ponerse en pruebas periódicas para que sean evaluados en cuanto a su efectividad y sean actualizados, según fuere necesario. Estas pruebas serán esenciales para promover el entendimiento y familiaridad entre el personal clave de sus roles y responsabilidades en el caso de una interrupción mayor.

Por otra parte, tanto la auditoría interna como la externa, deben evaluar la efectividad del programa de pruebas de institución, revisar los resultados de pruebas e informar sus hallazgos al comité de auditoría, la alta gerencia y la junta directiva, con el fin de que cualquier deficiencia encontrada sea subsanada oportunamente.

El Sistema de Control Interno – se estipula que las instituciones deberán contar con un sistema de control interno que cumpla con los requerimientos establecidos en la presente norma y en la normativa que regula la materia sobre control y auditoría interna[25]. Este sistema de control interno debe estar basado en los siguientes componentes:

- ✓ *Entorno de Control*, donde se deben tomar en cuenta los elementos relacionados con la integridad, los valores éticos, la capacidad de los empleados, la filosofía de la institución, el estilo de gestión, la asignación de la autoridad y sus responsabilidades, la organización y el desarrollo de los empleados y las orientaciones de la junta directiva;
- ✓ *Evaluación de la Riesgos,* enfocada primeramente en la identificación de los objetivos organizacionales y, posteriormente, en identificación y evaluación de los riesgos relevantes que puedan afectarle alcanzar dichos objetivos;
- ✓ *Actividades de Control,* entendiéndose por estos las políticas y procedimientos que ayuden asegurar que se tomen las medidas para limitar los riesgos que pueden afectar el alcance de los objetivos organizacionales; se refiere a las actividades como autorizaciones, verificaciones, conciliaciones, segregaciones de funciones y revisiones de rentabilidad operativa de la institución financiera;
- ✓ *Información y Comunicación,* señalando que se debe identificar, ordenar y comunicar oportunamente la información necesaria para que los empleados de la institución puedan cumplir con sus obligaciones;
- ✓ *Supervisión,* destacando que las instituciones financieras deben implementar procesos que conlleven realizar actividades de supervisión continua, evaluaciones periódicas o una combinación de ambas, para comprobar que sus sistemas de control interno se mantienen funcionando adecuadamente.

[25] La Norma sobre Control y Auditoría Interna fue aprobada por el Consejo Directivo de la SIBOIF el 01/09/2009.

Factores de Riesgo Operacional – en éste acápite la Norma sobre gestión de riesgo operacional, retoma los estándares internacionales, determinando los cuatro tipos de factores generadores del riesgo operacional y estableciendo que las instituciones financieras deberán gestionar apropiadamente los riesgos asociados a éstos:

a) Para mitigar el riesgo operacional relacionado con personas, se debe contar con: recursos humanos con las competencias idóneas para el desempeño de cada puesto, considerando no solo la experiencia profesional y la formación académica, sino también los valores, actitudes y habilidades; información actualizada de los recursos humanos, como organigramas y perfiles de puestos; comunicación fluida y constante; así como la capacitación permanente.
b) Para mitigar los riesgos asociados a procesos internos se debe: tener desarrolladas las políticas que comprenden el diseño de los procesos, descripción en secuencia lógica y ordenada de las actividades, tareas y controles, identificación de las personas responsables, monitoreo permanente de las políticas y procesos para actualizarlos y mejorarlos, difusión y comunicación de los procesos; contar con controles internos adecuados en cuanto a segregación de funciones para evitar las incompatibilidades; y tener inventariados y actualizados los procesos en funcionamiento, por ejemplo por tipo de proceso, responsable, productos y servicios que genera el proceso, clientes internos y externas, fecha de aprobación y actualización.
c) Para mitigar los riesgos por eventos externos tales como desastres naturales, incendios, atentados, actos delictivos, fallas en los servicios públicos, contingencias legales, se debe tener desarrolladas las políticas para la gestión de continuidad del negocio para cada uno de ellos.
d) Para mitigar los riesgos asociados con la tecnología de información, ya sea por interrupciones o fallas en los sistemas o fallas en los servicios provistos por terceros, se debe tener desarrollados los planes operativos y estratégicos actualizados, así como desarrollar políticas para aprobación de proyectos, propiedad intelectual, bases de datos, administración de software y hardware, outsourcing, administración de seguridad y gestión de continuidad del negocio.

Avances en la implementación de la Norma sobre gestión de riesgo operacional por parte de las instituciones financieras.

De acuerdo a las disposiciones transitorias de la Norma sobre gestión de riesgo operacional, las instituciones financieras tienen el plazo hasta el 31 de julio del año 2010 para adecuarse a los requerimientos establecidos, no obstante este plazo puede ser prorrogado por el Superintendente a solicitud individual debidamente justificada de las instituciones interesadas.

Así mismo, las instituciones financieras debían a más tardar los 60 días a partir de la entrada en vigencia de la presente norma, remitir al Superintendente sus planes de adecuación a las disposiciones contenidas en esta norma; éstos debían contener el diagnóstico preliminar de la situación actual de cada una de las instituciones que reflejaría los avances en el cumplimiento de los requerimientos establecidos en la norma, las acciones previstas para una adecuación total y el cronograma de las metas, así como los nombres de los funcionarios responsables del cumplimiento de dicho plan.

Según la entrevista realizada a la SIBOIF, las instituciones financieras han presentado sus planes de adecuación, sin embargo la mayoría de ellas han solicitado prorrogas para los puntos particulares.

El diagnóstico preliminar consolidado de la SIBOIF refleja un nivel de avances diferenciado:

- ✓ 4 bancos cuentan con la Unidad responsable de la gestión del riesgo operacional (UAIR);

- ✓ 1 banco reporta que cuenta con el sistema de control interno, la segregación de funciones adecuada y está gestionando sus riesgos asociados a tecnología de información. Informa que tiene en general un avance del 51 por ciento, estando aún en proceso la elaboración del sistema de gestión del riesgo operacional en cuanto a la aprobación de los objetivos, lineamientos y políticas (una vez identificados los riesgos operacionales comenzarán a desarrollar el Plan de Continuidad de Negocios); así como la elaboración y aprobación de los manuales de políticas y procedimientos, de organización y descripción de

funciones y de control de riesgo operacional (en el caso de manuales se estima el cumplimiento en diciembre del 2010). Así mismo, se está avanzando en la identificación de factores de riesgo operacional, se desarrolla la gestión de riesgos asociados a procesos internos, elaboración de políticas del diseño, control, actualización y seguimiento de los procesos y actualización de inventarios de los procesos. También se empezó a gestionar los riesgos asociados a personas (se revisarán las políticas con la GRHH) y eventos externos (se realizarán investigaciones y propuestas sobre el plan de contingencia y su presentación a la JD y Gerencia General). En éstos dos últimos se estima el cumplimiento al finalizar el mes de septiembre del año 2010.

- ✓ 1 banco informó que ya cuenta con la parte importante de la norma, pero solicitó el plazo adicional hasta el mes de diciembre del 2010, encontrándose pendiente lo siguiente: informes de evaluación por parte de auditoría interna con respecto al grado de cumplimiento de las políticas relacionadas con los factores de riesgo operacional; asignación de responsables que se encarguen de definir y autorizar de manera formal los accesos, cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos y definir políticas, procesos y procedimientos bajo mejores prácticas aplicables. Así mismo, está en proceso la implementación de segregación de funciones y lo relacionado con la gestión de riesgos asociados a personas (evaluación de los recursos humanos). También están abordando los aspectos relacionados con la gestión de riesgos asociados a eventos externos, como las contingencias legales y ocurrencia de desastres naturales, atentados y actos delictivos y la gestión de continuidad del negocio.

- ✓ 1 banco presentó su plan de adecuación general considerando los 4 factores del riesgo operacional, sin especificar los avances por artículo de la norma, reflejando que necesitaran 18 meses de adecuación para los procesos y el control interno, 12 meses para la gestión de los riesgos asociados con personas y 9 meses para terminar lo relacionado con el plan de continuidad del negocio.

- ✓ 1 banco informó que se han cumplido con la definición de responsabilidades y lineamientos para la gestión del riesgo operacional, sin embargo está pendiente la organización de gestión de riesgos asociados a procesos internos, específicamente relativo a: controles y procedimientos para la gestión del riesgo operacional, agrupándolos por líneas de negocio; elaboración y aprobación de los manuales de políticas y procedimientos, de organización y de control del riesgo operacional; así como gestión de riesgos asociados a personas y eventos externos. La fase piloto del modelo creado estaría probándose entre el mes de agosto del 2010 y febrero del 2011, para luego realizar el diagnóstico, mapeo de procesos, selección de indicadores y capacitaciones previstos a culminarse a finales del 2011.

- ✓ 1 banco informó que ya cuentan con la identificación de los procesos claves/ críticos y un proceso definido para evaluar y contabilizar las pérdidas operativas; así como ya tiene establecido un Comité de Control; desde el mes de junio de 2007 su Junta Directiva aprobó la política corporativa de evaluación y control de riesgo operacional; al finalizar el mes de diciembre se espera la finalización del proceso de adecuación, aprobándose los procedimientos.

- ✓ Restantes bancos han informado que se estima que el proceso de adecuación para el cumplimiento de la Norma sobre gestión del riesgo operacional culminará para el mes de diciembre del año en curso.

Las mayores dificultades de las instituciones financieras en esta etapa de adaptación a la presente norma están relacionadas con el cumplimiento de los lineamientos generales establecidos, los que en sí determinan la esencia de cómo gestionar el riesgo operacional. Sin embargo se espera que estas dificultades se superan; la identificación de eventos generadores de riesgo operacional servirá a las instituciones para detectar las debilidades dentro de sus organizaciones en cuanto a procesos y controles; la elaboración e implementación de las políticas y procedimientos como parte de una gestión efectiva les permitirá ordenar su funcionamiento, generar los reportes adecuados y oportunos; puestas en práctica las políticas de continuidad de negocio les

permitirán asegurar el funcionamiento y pronta recuperación en el caso de las futuras interrupciones; se minimizará el riesgo por subcontrataciones y de tecnología de información; trabajarán su propia base de datos para estimar pérdidas futuras a raíz de factores generadores del riesgo operacional, entre otros beneficios.

III. CONCLUSIONES

Independientemente que el riesgo ha estado siempre presente en las actividades bancarias, una serie de factores llevaron a que tanto la comunidad reguladora internacional como la industria financiera comenzaran manifestar una preocupación creciente por pérdidas provenientes de eventos de riesgo operacional. Primeramente el Comité de Supervisión Bancaria de Basilea en el año 2003 publicó una serie de principios sobre las buenas prácticas para la administración del riesgo operacional, sentando el precedente en el tratamiento integral del riesgo operacional como una categoría de riesgo. Posteriormente, en junio de 2004 se publicó Basilea II, donde se fija por primera vez un cargo de capital explícito para atender a las pérdidas provenientes de eventos de riesgo operacional.

En Nicaragua las disposiciones normativas dictadas por la Superintendencia de Bancos y de otras Instituciones Financieras, son de gran avance ya que sientan el inicio de la implementación de acciones concretas en materia de riesgo operacional. Estas toman como base las recomendaciones del Comité de Basilea, sin embargo en esta primera etapa únicamente relacionadas con la necesidad de contar con buenas prácticas de una efectiva gestión y supervisión del riesgo operacional, y aún no se les exige a las instituciones bancarias del sistema financiero nacional el capital para afrontar las posibles pérdidas operacionales futuras. Aunque sí, la Norma de gestión del riesgo operacional estipula que las instituciones apliquen las metodologías existentes para poder medir el riesgo operacional, conformando las bases de datos necesarias en función de las líneas de negocios, así como la implementación del sistema global de gestión del riesgo operacional sea agrupado por líneas de negocio; lo que indica que se está previendo por parte de la SIBOIF la generación del desarrollo de capacidades de

los bancos ante una eventual reforma a las normas, donde se les exigirá el aprovisionamiento de capital mínimo por riesgos operacionales.

La asimilación, preparación e implementación de la gestión del riesgo operacional en la práctica por parte de las instituciones financieras es un proceso complejo, minucioso y costoso, está siendo paulatino y se espera que este organizado e implementándose lo mas tardar para el año 2011.

Se puede concluir que una vez puesta en marcha por parte de los bancos la implementación de la Norma de la SIBOIF sobre gestión del riesgo operacional y otras complementarias aprobadas anteriormente, las instituciones financieras en Nicaragua gestionarán el riesgo operacional eficiente si:

- ✓ tendrán una definición clara sobre el riesgo operacional y lo reconocerán como un riesgo gestionable;
- ✓ existirá una función encargada de la administración de riesgo operacional (UAIRs) en cada una de las instituciones financieras;
- ✓ mantendrán las políticas para la administración de riesgo aprobadas por sus juntas directivas y altas gerencias;
- ✓ la estrategia de administración del riesgo operacional se implementará a través de toda estructura organizativa de cada una de las instituciones y todos los niveles del personal asumirán y comprenderán sus responsabilidades respecto a la administración de este riesgo;
- ✓ la estrategia de administración del riesgo operacional será consistente con el volumen y complejidad de sus actividades, teniendo en cuenta el nivel de tolerancia al riesgo en cada una de las instituciones;
- ✓ evaluarán el riesgo operacional inherente a todos los tipos de productos, actividades, procesos y sistemas;
- ✓ administrarán los riesgos operacionales considerando los impactos que pudieran provocar y la probabilidad de ocurrencia de los eventos;
- ✓ aseguran que antes de introducir nuevos productos, emprender nuevas actividades o establecer nuevos procesos y sistemas, se evaluará el riesgo operacional inherente;

- ✓ los sistemas de información permitirán hacer un monitoreo continuo de la exposición a los riesgos operacionales para servir en forma eficiente al proceso de toma de decisiones por parte de la junta directiva y alta gerencia;
- ✓ contarán con políticas para administrar los riesgos asociados a las actividades entregadas a terceros y llevar a cabo las verificaciones y monitoreos de estas actividades;
- ✓ contarán con la infraestructura tecnológica para el desarrollo normal de sus actividades;
- ✓ contarán con una estructura que permitirá administrar la seguridad de la información en términos de resguardar su confidencialidad, integridad y disponibilidad;
- ✓ tendrán elaborados y practicados los planes de continuidad del negocio y contingencia, considerando los diversos escenarios y supuestos que pudieran impedir que se cumplan sus objetivos;
- ✓ tendrán sistema de control interno eficiente;
- ✓ implementarán el proceso de control permanente sobre la incorporación de nuevas políticas, procesos y procedimientos, que permitan detectar y corregir sus eventuales deficiencias; entre otros.

En particular, considero que una vez establecido todo lo anterior se crearía una solida cultura de gestión de los riesgos operacionales, contribuyendo a una mejora de la eficiencia de los procesos, la rentabilidad y de la solidez y solvencia de las entidades financieras, arrojando en consecuencia, beneficios positivos para la estabilidad del sistema financiero en su conjunto. De tal manera que las instituciones financieras son las primeras interesadas en empezar a consolidarse en cuanto a gestión de los riesgos operacionales, invertir en la gestión, fortalecerse organizativamente, mejorar sus controles, lo que les permitirá ser más competitivos; por otra parte será necesaria la constancia en la gestión del riesgo operacional por parte de las instituciones para garantizar la continuidad de sus negocios.

IV. RECOMENDACIONES

La Superintendencia de Bancos y de Otras Instituciones Financieras, con sus estructuras correspondientes debe seguir implementando una supervisión adecuada de las instituciones financieras, y en particular dar seguimiento en el cumplimiento de las normas relacionadas con el riesgo operacional, con el fin de propiciar la estabilidad del sistema financiero nacional.

Las instituciones financieras del país, cumpliendo con el marco legal existente, deben desarrollar y perfeccionar sus sistemas de gestión de riesgo operacional, para garantizar la continuidad de sus negocios.

Una vez consolidada la gestión del riesgo operacional en la banca y contando con la serie de base de datos continuos, sería importante que la SIBOIF realizara cálculos de capital por riesgo operacional en cada uno de los bancos de acuerdo a los métodos de medición avanzados, con el fin de estimar el capital necesario para afrontar el riesgo operacional en cada uno de los bancos del sistema financiero nacional.

V. REFERENCIAS BIBLIOGRAFICAS

- ACCIONES Y VALORES, *"Manual de Administración de Riesgo Operativo"*, Bogotá, Junio de 2007.
- Arbeláez Juan Camilo, Franco Luis Ceferino, Betancur Cesar, Murillo Juan Guillermo, Gallego Paula Andrea, Henao Viviana María, Londoño Juana Andrea, Mejía Claudia Marcela, Palacio Diana Marcela, Salazar Elizabeth, Salazar Luisa Fernanda, Valderrama Natalia, Varela Diana Carolina, "Riesgo Operacional: Reto Actual de las Entidades Financieras", *Revista Ingenierías Universidad de Medellín 5(9)*: 97-110, Colombia, Julio – diciembre de 2006.
- Autoridad de Supervisión del Sistema Financiero de Bolivia (ASFI), *Boletín de Gestión de Riesgos No. 16 - Riesgo Operacional*, del viernes 10 de octubre del 2008.
- Cárdenas Santa María Patricia, "La gestión del riesgo operacional en Colombia: un tema de gran importancia en la agenda del sector financiero", *La Semana Económica, ASOBANCARIA,* No. 545 del 10 de maro de 2006.
- Carrillo Menéndez Santiago, "Basilea II: Una Mirada Crítica", *Colección Mediterráneo Económico No. 8,* pp.283-306.
- CEO Argentina, PricewaterhouseCoopers, Responsabilidad Social Corporativa, *"Riesgo Operacional"*, Editorial Hot Topics Año 3, Edición Especial, 2007.
- Comité de Supervisión Bancaria de Basilea, *"Documento Consultivo: El Nuevo Acuerdo de Capital de Basilea",* Banco de Pagos Internacionales (BPI), emitido para consulta hasta el 31 de mayo de 2001, Enero 2001.
- Comité de Supervisión Bancaria de Basilea, *"Buenas prácticas para la gestión y supervisión del riesgo operativo"*, Banco de Pagos Internacionales, Febrero 2003.
- Comité de Supervisión Bancaria de Basilea, *"Convergencia Internacional de Medidas y Normas de Capital"*, Banco de Pagos Internacionales (BPI), Marco Revisado, Junio de 2004.

- Compañía Aseguradora de Fianzas S.A. (Confianza), Gerencia de Riesgos, *Cartilla Guía de Riesgo Operativo: Capacitación en el Sistema de Administración de Riesgos Operacionales (SARO)*, Código GR-OD-01-01, noviembre de 2008.
- Cuéllar María Mercedes, "Gestión de riesgos en la banca: avances y desafíos", *La Semana Económica, ASOBANCARIA,* No. 633 del 30 de noviembre de 2007.
- Delfiner Miguel, Mangialavori Ana y Railhé Cristina, *"Buenas prácticas para la administración del riesgo operacional en entidades financieras"*, Enero 2007.
- Delfiner Miguel y Railhé Cristina, *"Técnicas cualitativas para la gestión del riesgo operacional"*, Octubre 2008.
- FEN, *"Manual de Riesgo Operativo"*, Bogotá, D.C. Octubre 17 de 2007.
- Gavilan Silvia G., Gerente de Consultas Normativas, Subgerencia General de Normas del Banco Central de la República Argentina (BCRA), *"Lineamientos para la gestión del riesgo operacional en las entidades financieras"*, 25 de abril del 2008.
- Gerencias de Régimen Informativo, Supervisión, Investigación y Planificación, Normativa y Auditoría de Sistemas, Banco Central de la República Argentina (BCRA), *"La gestión del riesgo operacional en el sistema financiero argentino"*, diciembre de 2009.
- HSBC México, Dirección de Análisis y Medición de Riesgo, "Ejemplos de Riesgo de Mercado y Operacional: casos Natwest, Long Term Capital Managment y Allied Irish Bank, *Gaceta de Basilea II*, No. 14 del año 2008.
- Huezo Castillo Ernesto, *"Curso de Supervisión y Regulación Bancaria"*, Coordinación Maestría y Postgrado en Economía y Desarrollo, Facultad de Ciencias Económicas y Empresariales, UCA, 2008.
- Jiménez Rodríguez Enrique José / Marín José Luís Martín, "El Nuevo Acuerdo de Basilea y la Gestión del Riesgo Operacional", *Universia Business Review,* tercer trimestre, número 007, Grupo Recoletos Comunication, Madrid, España, pp. 54-67.
- Martínez Castillo Carlos Alberto, "Basilea II, Retos y Oportunidades hacia una Mayor Armonización de la Regulación y Supervisión Financiera en el Siglo

XXI", *Gestión y Política Pública*, segundo semestre, año/vol.XVI, número 002, centro de Investigación y Docencia Económicas, A.C., D.F., México, pp.465-510.

- Méndez del Río Manuel A., "*Basilea II: La Carrera ha Empezado", Colección Mediterráneo Económico No. 8,* pp.307-317.
- Salinas Vicente, "La Solvencia de las Entidades Bancarias: El Nuevo Acuerdo de Capital, Basilea 2", *RVEH* No. 9 – III/2003, España, pp. 238-255.
- Nieto Giménez-Montesinos Ma.Ángeles, "El tratamiento del riesgo operacional en Basilea II", *Estabilidad Financiera No. 8*, Banco de España, pp. 165-185.
- Soto Quintana Antonio José, Stagg Marcial, Valiente Martínez María Rosa, "Gestión del riesgo operacional en la banca universal venezolana", *Revista Venezolana de Gerencia (RVG),* Año 14. No. 45, 2009, 96-109, Universidad de Zulia.
- Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF), Informe de consolidación de solicitudes de la banca sobre diagnóstico preliminar y plan de adecuación, junio del 2006.
- Ley No. 316, Ley de Superintendencia de Bancos y de Otras Instituciones Financieras, publicada en la Gaceta Diario Oficial No. 196 del 14/10/99.
- Ley No. 552, Reforma a la Ley No. 316, Ley de Superintendencia de Bancos y de Otras Instituciones Financieras, publicada en la Gaceta Diario Oficial No. 169 del 30/08/05.
- Ley No. 564, Reforma a la Ley No. 316, Ley de Superintendencia de Bancos y de Otras Instituciones Financieras, publicada en la Gaceta Diario Oficial No. 228 del 24/11/05.
- Ley No. 561, Ley General de Bancos, Instituciones Financieras No Bancarias y Grupos Financieros, publicada en la Gaceta Diario Oficial No. 232 del 30/11/05.
- Ley No. 564, Reforma a la Ley No. 316, Ley de Superintendencia de Bancos y de Otras Instituciones Financieras, publicada en la Gaceta Diario Oficial No. 58 del 22/03/06.

- Norma sobre la Contratación de Proveedores de Servicios para la Realización de Operaciones o Servicios a Favor de las Instituciones Financieras, Resolución No. CD-SIBOIF-421-1-MAY16-2006, del 16 de Mayo de 2006.
- Norma sobre la Administración Integral de Riesgos, Resolución No. CD-SIBOIF-423-1-MAY30-2006, del 30 de Mayo de 2006.
- Norma sobre Gestión de Riesgo Tecnológico, Resolución No. CD-SIBOIF-500-1-SEP19-2007, del 19 de Septiembre de 2007.
- Norma sobre Gestión de Riesgo Operacional, Resolución No. CD-SIBOIF-611-1-ENERO22-2010, del 22 de Enero de 2010.
- www.netconsul.com/riesgos/arbi.pdf
- www.revista-ays.com/DocsNum01/PersEmpresarial/DelPozo.pdf
- www.tuobra.unam.mx/obrasPDF/publicadas/040710174457.html
- www.bcra.gov.ar/comunica/cm020000pdf.asp?Texto=t-rieope.pdf
- www.scribd.com/doc/18769244/Editorial-0805
- www.idg.es/computerworld/Desastre-en-el-CPD.En-marcha-el-Plan-de-Contingenc/seccion-/articulo-9306
- www.elpais.com/articulo/sociedad/Bancos/empresas/fomentan/teletrabajo/nueva/gripe/elpepisoc/20090905elpepisoc_3/Tes
- http://fausto.cepeda.googlepages.com/BCPMayo2008.pd
- http://www.frbsf.org/publications/economics/letter/2002/el2002-02.html

VI. GLOSARIO

***Alta Gerencia**:* La persona que en las instituciones ocupe el cargo de ejecutivo principal (Presidente Ejecutivo, Director General, Director Ejecutivo, Gerente General), o sus equivalentes.

Base de Datos: Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de la institución.

Continuidad del negocio: Estado continuo e ininterrumpido de operación de un negocio.

Factores de Riesgo Operacional: Son las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operacional a nivel de la actividad o líneas de negocios, entre los cuales se encuentran: procesos internos, personas, eventos externos y tecnología de información.

***Gestión de Riesgo Operacional*:** Es el conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y revelar los riesgos operacionales a que se encuentran expuestas las instituciones financieras.

Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

Instituciones Financieras: Se refiere a los bancos y sociedades financieras que de acuerdo a la Ley General de Bancos pueden captar depósitos del público. Incluye a las sucursales de bancos y sociedades financieras extranjeras establecidas en Nicaragua.

Lineamientos a seguir: un conjunto de medidas, normas y objetivos que deben respetarse dentro de una organización.

Mejores Prácticas Aplicables: Se refiere a los marcos de referencia de control, estándares internacionales u otros estudios que ayuden a monitorear y mejorar las actividades críticas, aumentar el valor de negocio, y reducir riesgos, tales como; recomendaciones del Comité de Basilea, COSO, COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2, entre otros.

***Plan de Contingencia**:* Documento donde se detallan los procedimientos a seguir en caso de una contingencia, con el fin de no afectar el funcionamiento normal de la institución. Tiene como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

Plan de Continuidad del Negocio: Un componente de la gestión de continuidad del negocio. Es un plan de acción detallado que establece los procedimientos y sistemas necesarios por línea de negocio para continuar o restablecer las operaciones de una institución en el evento de una interrupción.

Políticas: Conjunto de prácticas establecidas por la junta directiva de la institución, por medio de las cuales se definen los cursos de acción a seguir por la administración.

***Procedimiento**:* Método o sistema estructurado para ejecutar instrucciones. Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de las cuales se asegura el cumplimiento de una función operativa.

Procesos: Conjunto de actividades, tareas y procedimientos organizados y repetibles.

***Procesos Críticos**:* Procesos considerados indispensables para la continuidad de las operaciones y servicios de la institución, cuyas falta o ejecución deficiente puede tener un impacto financiero significativo para la institución.

Riesgo de Tecnología de Información: Daño, interrupción, alteración o fallas derivadas del uso de la TI que soporta los procesos críticos de la Institución y que conlleve a una pérdida potencial.

Riesgo Legal: Pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la afectación por resoluciones administrativas o judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que las instituciones llevan a cabo.

Riesgo Operacional: Es el riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, las personas o los sistemas o por eventos externos. Esta definición incluye al riesgo legal y tecnológico, pero excluye el riesgo estratégico y reputacional.

Tecnología de Información (TI): Conjunto de recursos necesarios para procesar la información, convertirla, almacenarla, administrarla, transmitirla y encontrarla, tales

como: Hardware, Software, Sistemas de Información, Investigación Tecnológica, Redes Locales, Bases de Datos, Ingeniería de Software, Telecomunicaciones, Servicios y Organización de Informática.

Tercerización (Outsourcing): es un modelo estratégico de la gestión en donde los procesos del negocio se transfieren a otra compañía.

VII. ANEXOS

MULTAS IMPUESTAS POR LA INTENDENCIA DE BANCOS DE LA SIBOIF DE NICARAGUA(2007-2009)

ANEXO 1.

Año / Motivo	Entidad Sancionada	Sanción Impuesta (C$)
2007		**3080,733.16**
Incumplimientos derivados de resultados de Inspección In Situ		**2541,211.81**
	Financiera Fama S.A.	9,433.80
	Banco de Finanzas S.A.	187,144.00
	Banco de la Producción S.A.	559,744.31
	Consolidados de Seguros	576,358.20
	Banco de Crédito Centroamericano S.A.	370,852.00
	Financiera Arrendadora Centroamericana S. A.	193,788.00
	Banco Caley Dagnall S.A.	643,891.50
Incumplimiento al envío de información solicitada por		**74,809.00**
el Superintendente en el plazo establecido para dicha remisión		
	Consolidados de Seguros	56,308.50
	Banco de Finanzas S.A.	18,500.50
Incumplimiento a circular DS-DSES-1581-03-2007/VMUV		**55,198.15**
relacionada con la Central de Riesgo		
	Banco de Finanzas S.A.	9,235.40
	Banco de Crédito Centroamericano S.A.	9,218.15
	Banco Caley Dagnall S.A.	18,372.30
	Banco Procredit S.A.	18,372.30
Incumplimiento a instrucciones del Superintendente		**183,282.00**
	Banco de Crédito Centroamericano S.A.	183,282.00
Incumplimiento al Calendario Oficial de fechas de corte		**9,228.00**
y entrega de informes del primer semestre del 2007		
	Financiera Nicaraguense de Inversiones S.A.	9,228.00
Incumplimiento a lo estasblecido en los artos.3 numeral 9;		**18,162.30**
19 numeral 11 de la Ley 316 "Ley de la SIBOIF" y sus reformas		
Incumplimiento al artículo 113 numerales 1 y 5 párrafos		
segundo y tercero, de la Ley 561 "Ley General de Bancos,		
Instituciones Financieras No Bancarias y Grupos Financieros"		
	Banco Caley Dagnall S.A.	18,162.30
Incumplimiento al artículo 12 literal b, numeral 2, numeral v)		**90,376.00**
de la Norma sobre Imposición de Multas		
	Banco de la Producción S.A.	90,376.00
Incumplimiento al artículo 23 literal B) de la Norma sobre		**36,290.80**
Supervisión Consolidada de los Grupos Financieros		
	Banco de Finanzas S.A.	36,290.80
Incumplimiento a lo establecido en el Manual Unico de Cuentas		**9,024.30**
	Banco de Crédito Centroamericano S.A.	9,024.30
Incumplimiento al artículo 44 de la Norma sobre Evaluación y		**18,029.30**
Clasificación de Activos		
	Consolidados de Seguros	9,024.30
	Banco de la Producción S.A.	9,005.00
Incumplimiento al Artículo 37 de la Ley 561 "Ley General de Bancos,		**9,024.30**
Instituciones Financieras No Bancarias y Grupos Financieros"		
	Consolidados de Seguros	9,024.30
Incumplimiento al artículo 15 de la Norma sobre Oficiales de		**36,097.20**
Cumplimiento		
	Banco de la Producción S.A.	18,048.60
	Consolidados de Seguros	18,048.60

MULTAS IMPUESTAS POR LA INTENDENCIA DE BANCOS DE LA SIBOIF DE NICARAGUA(2007-2009)

ANEXO 1.

Año / Motivo	Entidad Sancionada	Sanción Impuesta (C$)
2008		**1136,362.59**
Incumplimiento al envío de información solicitada por		**268,362.60**
el Superintendente en el plazo establecido para dicha remisión		
	Banco de Crédito Centroamericano S.A.	9,824.00
	Banco de Crédito Centroamericano S.A.	9,824.00
	Consolidados de Seguros	191,771.00
	Banco de la Producción S.A.	56,943.60
Incumplimiento a lo establecido en Circular DS-VIB-0237-02-08-VMUV,		**19,520.10**
Calendario Oficial de fechs de Entrega de la Información Requerida		
por la SIBOIF, correspondiente al primer semestre del 2008		
	Banco de Crédito Centroamericano S.A.	19,520.10
Incumplimiento al Artículo 56 de la Ley 561 "Ley General de Bancos,		**194,629.00**
Instituciones Financieras No Bancarias y Grupos Financieros" respecto al		
exceso en el límite de concentración de crédito con partes no relacionadas		
	Financiera Fama S.A.	194,629.00
Incumplimiento al arto. 8, inciso c) de la Norma sobre Límites de Depósitos		**9,719.80**
e Inversiones		
	Banco de Finanzas S.A.	9,719.80
Incumplimiento al arto. 14 de la "Norma sobre Límites de Depósitos		**9,566.09**
e Inversiones"		
	Banco de Crédito Centroamericano S.A.	9,566.09
Incumplimiento a lo establecido en el Manual Unico de Cuentas		**9,721.10**
	Banco Caley Dagnall S.A.	9,721.10
Incumplimiento a la Norma sobre Límites de Concentración		**96,411.00**
	Financiera Fama S.A.	96,411.00
Incumplimiento al arto.13, inciso b) de la Norma sobre Límites de		**60,385.80**
Concentración		
	Banco Citibank de Nicaragua S.A.	60,385.80
Incumplimiento al Artículo 57, numeral 5, de la Ley 561 "Ley General de		**28,920.70**
Bancos, Instituciones Financieras No Bancarias y Grupos Financieros"		
	Banco Procredit S.A.	9,633.40
	Consolidados de Seguros	19,287.30
Incumplimientos derivados de resultados de Inspección In Situ		**439,126.40**
	Banco de Crédito Centroamericano S.A.	57,927.40
	Banco de América Central S.A.	191,184.00
	Banco Procredit S.A.	190,015.00
2009		**1822,658.22**
Incumplimiento al envío de información solicitada por		**10,371.60**
el Superintendente en el plazo establecido para dicha remisión		
	Banco de Finanzas S.A.	10,371.60
Incumplimiento a la Norma sobre Contratación de Proveedores de		**41,397.80**
Servicios para la Realización de Operaciones o Servicios a favor de las		
instituciones financieras, contenida en Resolución CD-SIBOIF-421-1-16/05/06		
	Banco de Finanzas S.A.	41,397.80
Incumplimiento a la Norma sobre Gestión de Riesgo Crediticio y a la Norma		**164,420.55**
sobre Contratación de Proveedores de Servicios para la Realización de		
Operaciones o Servicios a favor de las instituciones financieras		

MULTAS IMPUESTAS POR LA INTENDENCIA DE BANCOS DE LA SIBOIF DE NICARAGUA(2007-2009)

ANEXO 1.

Año / Motivo	Entidad Sancionada	Sanción Impuesta (C$)
	Banco de Crédito Centroamericano S.A.	164,420.55
Incumplimiento en la entrega de información en la fecha establecida en		**20,508.90**
Calendario Oficial de Entrega de Información del primer semestre 2009		
	Banco de Crédito Centroamericano S.A.	20,508.90
Incumplimiento en el envío de información requerrida por		**20,685.10**
el Superintendente en el plazo establecido para su remisión, disposición		
contenida en el arto. 3 numeral 9, arto. 19 numeral 11 de la Ley 316		
"Ley de la SIBOIF" y arto. 113 numeral 1 y 5 párrafos segundo y tercero		
de la Ley 561 "Ley General de Bancos,		
Instituciones Financieras No Bancarias y Grupos Financieros"		
	Banco Citibank de Nicaragua S.A.	20,685.10
Incumplimiento del artículo 4 de la Norma sobre Funcionamiento y		**20,435.00**
Procesamiento de Datos de la Central de Riesgo		
	Banco Citibank de Nicaragua S.A.	20,435.00
Incumplimiento al artículo 13, inciso b) de la Norma sobre Límites de		**121,404.60**
Concentración		
	Banco de Finanzas S.A.	61,018.80
	Banco Citibank de Nicaragua S.A.	60,385.80
Incumplimientos derivados de resultados de Inspección In Situ		**1011,692.50**
	Banco de la Producción S.A.	505,710.00
	Banco Citibank de Nicaragua S.A.	505,982.50
Incumplimiento en el establecimiento de las obligaciones recíprocas en		**200,769.07**
los instrumentos contractuales de créditos		
	Banco de la Producción S.A.	200,769.07
Incumplimiento en el envío de información requerrida por		**210,973.10**
el Superintendente en el plazo establecido para su remisión, disposición		
contenida en el arto. 3 numeral 9, arto. 19 numeral 11 de la Ley 316		
	Banco de la Producción S.A.	10,036.10
	Banco de Exito S.A.	200,937.00
TOTAL GENERAL MULTAS (2007-2009)		**6039,753.97**

ANEXO 7 DE LA BCBS SOBRE CLASIFICACION PORMENORIZADA DE TIPOS DE EVENTOS DE PERDIDAS

ANEXO 2.

Categorías de Tipos de Eventos (Nivel)	Definición	Categorías (Nivel 2)	Ejemplos de Actividades (Nivel 3)
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa	Actividades no autorizadas	Operaciones no reveladas (intencionalmente) Operaciones no autorizadas (con perdidas pecuniarias) Valoración erróneas de posiciones (intencional)
		Hurto y fraude	Fraude / fraude crediticio / depósitos sin valor Hurto / extorsión / malversación / robo Apropiación indebida de activos Destrucción dolosa de activos Falsificación Utilización de Cheques sin fondos Contrabando Apropiación de cuentas, de identidad, etc. Incumplimiento / evasión de impuestos (Intencional) Soborno / Cohecho Abuso de información privilegiada (no a favor de la empresa)
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero	Hurto y fraude	Hurto / robo Falsificación Utilización de cheques sin fondos
		Seguridad de los sistemas	Daños por ataques informáticos Robo de información (con perdidas pecuniarias)
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad / discriminación	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos. Organización laboral
		Higiene y Seguridad en el trabajo	Responsabilidad en general (resbalones, etc.) Casos relacionados con las normas de higiene y seguridad en el trabajo Indemnización a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación
Clientes, productos y practicas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación) o de la naturaleza o diseño de un producto	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas Aspectos de adecuación / divulgación de información (know your customer KYC, etc.) Quebramiento de la privacidad de información sobre clientes minoristas Quebramiento de la privacidad Ventas agresivas Confusión de cuentas Abuso de información confidencial Responsabilidad del prestamista
		Prácticas empresariales o de mercado improcedentes	Prácticas restrictivas de la competencias Prácticas comerciales / de mercado improcedentes Manipulación del mercado Abuso de información privilegiadas (a favor de la empresa) Actividades no autorizadas Blanqueo de dinero
		Productos defectuosos	Defectos del producto (no autorizado, etc.) Error de los modelos
		Selección, patrocinio y riesgo	Ausencia de investigación a clientes conforme a las directrices Superación de los limites de riesgo frente a clientes
		Actividades de asesoramiento	Litigio sobre resultados de las actividades de asesoramiento
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Desastres y otros acontecimientos	Pérdidas por desastres naturales Pérdidas humanas por causas externas (terrorismo, vandalismo)
Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas	Sistemas	Hardware Software Telecomunicaciones Interrupción / incidencias en le suministro

ANEXO 7 DE LA BCBS SOBRE CLASIFICACION PORMENORIZADA DE TIPOS DE EVENTOS DE PERDIDAS

ANEXO 2.

Categorías de Tipos de Eventos (Nivel)	Definición	Categorías (Nivel 2)	Ejemplos de Actividades (Nivel 3)
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	Comunicación defectuosa Errores de introducción de datos, mantenimiento o descarga Incumplimiento de plazos o de responsabilidades Ejecución errónea de modelos / sistemas Error contable / atribución a entidades erróneas Errores en otras tareas Fallo en la entrega Fallo en la gestión del colateral Mantenimiento de datos de referencia
		Seguimiento y presentación de informes	Incumplimiento de la obligación de informar Inexactitud de informes externos (con generación de perdidas)
		Aceptación de clientes y documentación	Inexistencias de autorizaciones / rechazos de clientes Documentos jurídicos inexistentes / incompletos
		Gestión de cuentas de clientes	Acceso no autorizado a cuentas Registros incorrectos de clientes (con generación de perdidas) pérdida o daño de activos de clientes por negligencia
		Contrapartes comerciales	Fallos de contrapartes distintas de clientes otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	Subcontratación Litigios con distribuidores

ANEXO 6 DE LA BCBS SOBRE ASIGNACION DE LAS LINEAS DE NEGOCIO

ANEXO 3.

Nivel 1	Nivel 2	Grupos de Actividades
Finanzas corporativas	Finanzas corporativas Finanzas de administraciones locales / publicas Bancas de inversión Servicios de asesoramiento	Fusiones y adquisiciones, Suscripción de emisiones, privatizaciones, titulización, servicio de estudios, deuda (pública, alto rendimiento), acciones, sindicaciones, ofertas públicas, iníciales, colocaciones privadas en mercados secundarios
Negociación y ventas	Ventas Creación de mercado Posiciones propias Tesorerías	Rentas fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda, intermediación unificada (prime brokerage)
Banca minorista	Banca minorista	Préstamos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarias
	Banca privada	préstamos y depósitos de particulares, servicios bancarios, fideicomisos y testamentarias, y asesoramiento de inversión
	Servicios de tarjetas	Tarjetas de empresa / comerciales, de marca privada y minoristas
Banca comercial	Banca comercial	Financiación de proyectos, bienes raíces, financiación de exportaciones financiación comercial, factoring, arrendamiento financiero, préstamo, garantías, letras de cambio
Pago y liquidación	Clientes Externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación
Servicios de agencia	Custodia	Contratos de plica, certificados de depósitos, operaciones de sociedades (clientes) para préstamo de valores
	Agencia para empresas	Agentes de emisiones y pagos
	Fideicomisos de empresas	
Administración de activos	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrados, abiertos participaciones accionariales
	Administración no Discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable
Intermediación minorista	Intermediación minorista	Ejecución y servicios completo